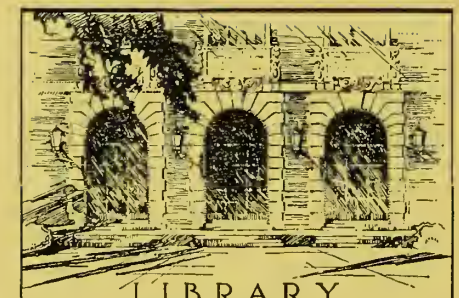

Report No. 263

ON THE USE OF FINITE FIELD BASED MODELING IN POLYNOMIAL MANIPULATION

by

Stephen J. Nuspl

June 1, 1968

DEPARTMENT OF COMPUTER SCIENCE · UNIVERSITY OF ILLINOIS · URBANA, ILLINOIS

Report No. 263

ON THE USE OF FINITE FIELD BASED MODELING IN POLYNOMIAL MANIPULATION*

by

Stephen J. Nuspl

June 1, 1968

Department of Computer Science
University of Illinois
Urbana, Illinois 61801

* This work was submitted in partial fulfillment of the Doctor of Philosophy in Electrical Engineering and was supported in part by the National Science Foundation under Grant No. NSF-GP-4636.

ON THE USE OF FINITE FIELD BASED MODELING IN POLYNOMIAL MANIPULATION

Stephen John Nuspl, Ph.D.
Department of Electrical Engineering
University of Illinois, 1968

A major hindrance to the manipulation of polynomials by a computer is the rapid growth of the polynomial coefficients during the application of some frequently used algorithms. The methods presented in this thesis to try to alleviate this problem and to increase the efficiency of polynomial manipulation are based on the use of algebraic redundancy.

Let I_0 be the set of all integers and I_{i+1} be the adjunction of I_i consisting of the set of all polynomials in x_{i+1} with coefficients in I_i. Let F_0 be a field of order p_0 where p_0 is a prime in I_0. The extension field F_{j+1} is defined to be the set of residues in $F_j[x_{j+1}]$ modulo p_{j+1}, a monic irreducible polynomial in $F_j[x_{j+1}]$. The sets I_i are defined as the modeled domains and the sets F_j and their adjunctions as the model domains. A modeling function which maps any element of a modeled domain into any one of the model domains in defined and shown to be a homomorphism.

Some of the models are capable of retaining the degree information of selected indeterminates in the modeled polynomials. A virtual degree augmentation is added to the

model and its algebraic treatment is developed in such a way that it is able to detect when a model polynomial has the same degree as the modeled polynomial without looking at the latter. A major result based on the augmented modeling is the model conclusive g.c.d. theorem which gives the conditions under which two polynomials can be shown relatively prime by performing the g.c.d. algorithm only on their models. Since model domains in which the coefficients are finite field elements can be chosen, the computational effort required can in many cases be orders of magnitude less than if the g.c.d. algorithm were applied directly to the modeled polynomials. Further applications of modeling are discussed but not developed to any depth.

ACKNOWLEDGMENT

The author would like to thank his advisor, Professor J. E. Robertson, for his guidance, encouragement and support given during the development of the ideas in this dissertation and for his suggestions leading to the improvement of its presentation.

Thanks are due to Mrs. G. Polizzotti for her patience and meticulous care in the preparation of the manuscript.

TABLE OF CONTENTS

CHAPTER I INTRODUCTION

The increasing use of the computer as an aid in algebraic manipulation makes it desirable to study techniques by which the speed of performing a manipulation is increased and the amount of physical equipment required during the manipulation is decreased. Of central importance are techniques by which polynomials in several variables are handled since most problems eventually filter down to a total description by polynomials or a description in which polynomials play a key role. In most practical cases the polynomials are defined over the integral domain of integers and consequently it is algorithms in these polynomial domains which should be optimized for speed and minimality of equipment.

The method proposed in this thesis to accomplish this is to add to the internal representation of the polynomial redundant information in such a way that the redundancy may be used to determine some desired properties of a polynomial without requiring that the entire polynomial be scanned for the property. For example, we may have two polynomials in a number of variables and we may wish to ask the question "Is polynomial 'a' identical to polynomial 'b' in the sense that if both are put into the same canonical form and ordering, for every term in 'a' there is an identical term in 'b'?" The straight forward way of answering this question is to put 'a' and 'b' into the same canonical form and compare them

term-by-term until a mismatch occurs or until the terms are exhausted. When such an algorithm has a very high probability of producing the answer "no" and if the much more concise redundancy is able to state conclusively that "no" is the answer, considerable total time can be saved by first trying to answer the question only with the redundancy. Then the actual polynomials must be used only if the redundancy does not produce a conclusive "no". In either case the answer will be the same as when only the actual polynomials are used but because of the high probability of a "no" the comparative average time for answering the question can be orders of magnitude lower when the redundancy is used.

Of particular interest is redundant information which retains some of the structure of the polynomials. When operations are performed on the redundancy and the result gives some information about the effect of applying the equivalent operations on the actual polynomials, the redundancy can be thought of as being a "model" of the actual polynomial. Since this will be the case in the development of this thesis, we will define the sets of all polynomials over the integral domain of all integers as the "modeled domains", the sets of all models as the "model domains" and the process of mapping a modeled polynomial into its model as a "modeling function".

The modeling used in this thesis is based on finite fields and their adjunctions in the sense that the model

domains are either finite fields or adjunctions of finite fields. The usefulness of this particular type of modeling stems primarily from the fact that the modeling functions which will be defined are homomorphisms from the modeled domains into the model domains which produces the desired effect of preserving some of the structure during the modeling. It will be shown that some of the modelings which will be defined have the additional property of being capable of retaining the degree information of selected variables and burying the rest in the finite field coefficients of these variables. The practical significance of this is that the degree information of the selected variables can be used for decisions in algorithms while at the same time the coefficients are finite field elements which implies that they are automatically restricted in size. Normally the problem in polynomial manipulation is that the coefficients grow so rapidly during the application of an algorithm that it is impractical to work with other than almost trivial polynomials in a few variables even when a very fast computer is used to perform the manipulation.

The only other effort known to the author in which finite field theory was used as an aid in algebraic manipulation is ref. (8) by W. A. Martin. On the one hand his approach was much more ambitious than that contained in this thesis since the modeling was extended to functions of a complex

variable. However, his models were restricted to take on values only in a prime field which resulted in the loss of all degree information in the models. It is precisely the preservation of this information which gives so much power to the modeling developed here even though it is restricted to polynomials over integers. Finite field theory has been found useful in determining the existence of solutions of equations, so it is not too surprising that the same theory can also play an important role in practical manipulative work with polynomials.

The development of the modeling is first started in Chapter 2 with the review of some concepts in modern algebra which are later required, a rigorous definition of the modeled and model domains and some relations among these domains. The modeling functions are defined and proven homomorphisms in Chapter 3. The detailed homomorphism proofs are included mainly for completeness; they need not be studied in order to understand the modelings. Finally, a summary which should help to unify and to make more understandable the relations between the various modeling functions is presented in section 3.7.

Chapter 4 introduces the additional concept of a virtual degree augmentation to the models. A set of operations defined on the augmented domains are developed in sufficient depth to be able to arrive at an adequate set of functions

which permit us to define a greatest common divisor (g.c.d.) algorithm which operates on elements in the model domains. It is then shown by the "model conclusive g.c.d. theorem" that two polynomials can be shown to be relatively prime under specified conditions by using only elements in the model domains during the computation. The practical significance of this is demonstrated with a set of examples.

In Chapter 5 some practical aspects of operations in the prime subfield and in other model domains are briefly considered. The appendix includes an example of a complete set of models for a polynomial in 3 variables and a tabulation of a set of primes with selected properties.

CHAPTER II BACKGROUND, POLYNOMIAL DEFINITIONS, DOMAINS

2.1 Introduction

In order to define the polynomial modeling process rigorously it is first necessary to review the definition of a polynomial ring and the operations which are related to the modeling. The required theory is based on concepts in modern algebra some of which will be stated in section 2.2. Much of the material is very elementary for someone well acquainted with algebra, but its inclusion is necessary in some cases for the explicit referencing of well-known theorems and in other cases it is used as a means of defining the notation intrinsically. For example, the definition of a group includes the normally used existential quantifier ($\exists$), the universal quantifier ($\forall$) and the symbol ($\ni$) standing for "such that". The reader not familiar with a concept or symbol used should consult one of the references (1), (10), (11).

2.2 Notation, Conventions, Polynomial Rings

Let $\{S,O\}$ be a monoid in which S is a set of elements closed under the binary associative operation $O : S \times S \longrightarrow S$. Let 0 and 1 represent the identity element in S when the operation O is respectively additive and multiplicative. The sum symbol, $\sum O$ will then be defined as follows:

For $a_i \in S$, $\bigcirc_{i=0}^{0}(a_i) = a_0$; $\bigcirc_{i=0}^{n+1}(a_i) = (\bigcirc_{i=0}^{n}(a_i)) \bigcirc a_{n+1}$

for $n \geq 1$.

When $\bigcirc$ is additive we make the additional convention: for

$a \in S$, $n \geq 0$ define $na = \bigcirc_{i=0}^{n}(a_i)$ where $a_0 = 0$, $a_i = a$ $0 < i$

When $\bigcirc$ is multiplicative we define

$$a^n = \bigcirc_{i=0}^{n}(a_i) \quad \text{where} \quad \begin{cases} a_0 = 1 \\ a_i = a \quad 0 < i \end{cases}.$$

It is immediately apparent that for $m \geq 0$, $n \geq 0$

$ma \bigcirc na = (m+n)a$ when $\bigcirc$ is additive

$a^m \bigcirc a^n = a^{m+n}$ when $\bigcirc$ is multiplicative.

Definition: $\{G, \bigcirc\}$ is a group if G is a non-empty set and $\bigcirc$ is a binary operation on the cartesian product $G \times G$ with the following properties:

<2.2.01>

1. $\bigcirc : G \times G \longrightarrow G$ (Closure)
2. $a, b, c \in G \Rightarrow a \bigcirc (b \bigcirc c) = (a \bigcirc b) \bigcirc c$ (Associativity)
3. $\exists\, e \in G \ni \forall\, a \in G,\ a \bigcirc e = a$
4. $\forall\, a \in G,\ \exists\, b \in G \ni a \bigcirc b = e$

Definition: <2.2.03> $\{R,\oplus,\odot\}$ is a ring if $\{R,\oplus\}$ is a commutative group and $\odot$ is a binary operation on $R \times R$ with the properties:

1. $\odot : R \times R \longrightarrow R$
2. $a,b,c \in R \Rightarrow a \odot (b \odot c) = (a \odot b) \odot c$
3. $a,b,c \in R \Rightarrow a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$
   and $(a \oplus b) \odot c = (a \odot c) \oplus (b \odot c)$

The ring $\{R,\oplus,\odot\}$ will be referred to as "the ring R with respect to the operations $\oplus$, $\odot$" or, when it is understood that R forms a ring with respect to the operations $\oplus$, $\odot$ simply as "the ring R" or "R".

Definition: <2.2.04> Let $\{R,+,\cdot\}$, $\{R_1,\oplus,\odot\}$ be rings and $\lambda : R \longrightarrow R_1$. Then λ is a ring homomorphism from R into R_1 if $\forall a,b \in R$, $a\lambda \oplus b\lambda = (a + b)\lambda$; $a\lambda \odot b\lambda = (a \cdot b)\lambda$. Under these conditions we denote λ by $\lambda : R \xrightarrow{H} R_1$.

Definition: <2.2.05> e is called the multiplicative identity or unit of R if $e \odot a = a \odot e = a$ for each a in R. If e is in R, R is said to be a ring with an identity.

Definition: $Z_0^+ = \{i \mid i \text{ is an integer and } 0 \leq i\}$
<2.2.06>

Definition: An infinite R-sequence is defined by the fol-
<2.2.07> lowing: Let $\{R,\oplus,\odot\}$ be a ring with identity. Let 0, 1 be the zero and unit in R. An infinite R-sequence is then defined to be a function $f : Z_0^+ \longrightarrow R$ where $(i)f = r_i$ with $i \in Z_0^+$, $r_i \in R$. f is denoted by $f = (r_0,r_1,r_2,\ldots,r_i,\ldots)$. r_i is sometimes called the i'th coefficient or i'th component of f.

Definition: $R_1 = \{u \mid u$ is an infinite R-sequence;
<2.2.08> $u = (u_0,u_1,\ldots)$ and $\exists\, n \ni \forall\, i > n,\ u_i = 0\}$.
The last condition is equivalent to saying that only a finite number of the components of u are not the zero element in R.

Definition: Let $u,v \in R_1$. $u = (u_0,u_1,u_2,\ldots)$,
<2.2.09> $v = (v_0,v_1,v_2,\ldots)$ where $u_i,v_i \in R$. We define the binary operators $\underline{\oplus}$, $\underline{\odot}$ as follows:

$$\underline{\oplus} : R_1 \times R_1 \longrightarrow R_1 \text{ where } u \underline{\oplus} v = (u_0 \oplus b_0, u_1 \oplus v_1, \ldots)$$
$$\underline{\odot} : R_1 \times R_1 \longrightarrow R_1 \text{ where } u \underline{\odot} v = (c_0,c_1,c_2,\ldots)$$
$$\text{and } c_i = \sum_{j=0}^{i} \oplus\, (u_j \odot v_{i-j}) = \sum_{j+k=i} \oplus\, (u_j \odot v_k)$$

Theorem: <2.2.10> $\{R_1, \underline{\oplus}, \underline{\odot}\}$ is a ring with identity in which the zero element is $\underline{0} = (0,0,0,\ldots)$ and the unit is $\underline{1} = (1,0,0,\ldots)$.

Definition: <2.2.11> $\underline{R} = \{u \mid u = (u_0,0,0,\ldots);\ u_0 \in R,\ u \in R_1\}$

Theorem: <2.2.12> $\underline{R} \subset R_1$ and $\{\underline{R}, \underline{\oplus}, \underline{\odot}\} \cong \{R, \oplus, \odot\}$ where $\cong$ denotes ring isomorphism and with the isomorphism defined by the function $\lambda : R \longrightarrow \underline{R}$ where $a \in R \Rightarrow a\lambda = (a,0,0,\ldots)$. The isomorphism λ will sometimes be referred to as an embedding of R in R_1.

Definition: <2.2.13> Scalar multiplication is defined to be the binary operation $\underset{\circ}{\odot} : R \times R_1 \longrightarrow R_1$ where $a \in R,\ u \in R_1 \Rightarrow a \underset{\circ}{\odot} u = (a \odot u_0, a \odot u_1, \ldots)$.

Theorem: <2.2.14> The complex $\{\{R, \oplus, \odot\}, \{R_1, \underline{\oplus}\}, \underset{\circ}{\odot}\}$ is a vector space over R and $\{x^0, x^1, x^2, \ldots\}$ is a set of basis elements when $x = (0,1,0,0,\ldots) \in R_1$.

Proof: The vector space properties are readily proven; of interest to us is the fact that $\{x^0, x^1, \ldots\}$ is a set of basis elements. By our definition of exponentiation,

$$x^0 = \sum_{i=0}^{0} \underset{\circ}{\odot} (x) = \underline{1};\quad x^j = \sum_{i=0}^{j} \underset{\circ}{\odot} (x) = (0,0,\ldots,1,0,\ldots)$$

where the 1 is in the j-th component position of x^j. For $u \in R_1$, $u = (u_0, u_1, u_2, \ldots)$, $u_i \in R$, u can be expressed as $u = \sum_{i=0}^{n} \underline{\oplus} (u_i \odot x^i)$. It follows that $\{x^0, x^1, \ldots\}$ is a set of basis elements for R_1.

<2.2.15> **Definition:** If $s \in R_1$ and $a \odot s = s \odot a \quad \forall a \in R$, s is said to be a scalar over R. Since R is commutative every element in R_1 is a scalar and of particular importance, x is a scalar.

<2.2.16> **Definition:** v is said to be algebraic over R if $v \in R_1$ and $\exists n, a_i, 0 \leq i \leq n$ such that at least some $a_i \neq 0$ and that $\sum_{i=0}^{n} \underline{\oplus} (a_i \odot v^i) = \underline{0}$.

<2.2.17> **Definition:** v is said to be an indeterminate over R if $v \in R_1$ and v is not algebraic over R. We note that x is an indeterminate over R.

<2.2.18> **Definition:** Let $y \in R_1$ be an indeterminate over R. Then $u = \sum_{i=0}^{n} \underline{\oplus} (u_i \odot y^i)$ for $u_i \in R$, $n \in Z_0^+$ is said to be a polynomial in y over R. The set of all such expressions is denoted by R[y].

From the definition of R[y] and the previous observation that $\{x^0, x^1, x^2, \ldots\}$ forms a basis for R_1

we can conclude that $R[x] = R_1$. Also, for some other indeterminate, z, over R we can see that $R[z] \cong R[x]$ by defining the function $\lambda : R[z] \longrightarrow R[x]$ where $u = \sum_{i=0}^{n} \underline{\oplus} (u_i \underline{\odot} z^i) \in R[z]$ and $u\lambda = \sum_{i=0}^{n} \underline{\oplus} (u_i \underline{\odot} x^i)$. λ is easily shown to be an isomorphism from $R[z]$ onto $R[x]$.

<2.2.19> **Definition:** Let $u \in R[x]$. Then it is known that there exists an n such that for all $i > n$, $u_i = 0$ where u_i is the i-th coefficient of u. If $u_n \neq 0$, u is said to have degree $\deg(u) = n$. If $u_n = 0$ or if it is not known whether $u = 0$ or not, u is said to have virtual degree n. The degree of $\underline{0} = \sum_{i=0}^{0} (0 \cdot x^i)$ is defined to be $-\infty$.

<2.2.20> **Definition:** Let $n = \deg(u)$, $u_n \neq 0$. Then u_n is called the leading coefficient of u and $\mathscr{l}(u) = u_n$.

<2.2.21> **Definition:** Let $u \in R[x]$. Then u is said to be monic if $\mathscr{l}(u) = 1$.

If $u, v \in R[x]$, then $\deg(u \underline{\oplus} v) \leq \max(\deg(u), \deg(v))$ and $\deg(u \underline{\odot} v) \leq \deg(u) + \deg(v)$. Since $R[x]$ may have divisors of zero, the inequality in the latter is necessary. However, we will be mostly concerned with integral domains, in which case we can state

$$\deg (u \underline{\odot} v) = \deg(u) + \deg(v)$$

Notation Convention: <2.2.30> Up to this point the vector operator symbols have been kept separate from the ring operator symbols in formulas. The normal convention is to omit or replace the vector and scalar operators with the ring operator symbols or with concatenation for multiplication when no confusion results. Since we will be working with an arbitrarily large number of integral domains and finite fields each with its own set of operators, we must adopt some of these conventions for compactness in expressions, but since each of the finite fields will require a different symbol for its operators we must take more than usual care in making these notation conventions.

As examples, let $u,v \in R[x]$. $u = \sum_{k=0}^{K} \underline{\oplus} (u_k \dot{\odot} x^k)$, $v = \sum_{m=0}^{M} \underline{\oplus} (v_m \dot{\odot} x^m)$. Define $N = \max(M,K)$

Then
$$u \underline{\oplus} v = \sum_{n=0}^{N} \underline{\oplus} ((u_n \oplus v_n) \dot{\odot} x^n)$$

$$u \underline{\odot} v = \sum_{n=0}^{K+M} \underline{\oplus} ((\sum_{n=k+m} \oplus (u_k \odot v_m)) \dot{\odot} x^n)$$

We now make the convention that the scalar product operator symbol $\dot{\odot}$ will be omitted and that the vector operator symbol $\underline{\odot}$ will be replaced by the ring operator $\odot$. The above

formulas now reduce to $u = \sum_{k=0}^{K} \oplus (u_k x^k)$, $v = \sum_{m=0}^{M} \oplus (v_m x^m)$

$$u \oplus v = \sum_{n=0}^{N} \oplus ((u_n \oplus v_n)x^n)$$

$$u \odot v = \sum_{n=0}^{K+M} \oplus \Big(\sum_{n=k+m} \oplus (u_k \odot v_m)\Big)x^n)$$

In addition we will also sometimes omit the $\oplus$ symbol following a summation symbol when the summation is only a formal representation of a polynomial. For example three formal representations of the polynomial u would be

$$u = (u_0, u_1, u_2, \ldots\ldots) = \sum_{k=0}^{K} \oplus (u_k x^k) = \sum_{k=0}^{K} u_k x^k$$

However, the subterm $\sum_{n=k+m} \oplus (u_k \odot v_m)$ cannot be reduced to $\sum_{n=k+m} (u_k \odot v_m)$ since in this particular case the symbol $\sum \oplus$ represents an actual summation using the ring operator $\oplus$.

2.3 Polynomials over Integral Domains, Finite Fields

<2.3.01> Definition: An integral domain is a commutative ring with a unit and with no divisors of zero.

Let $\{I, +, \cdot\}$ be an integral domain. Then $I[x]$ is the ring of polynomials in the indeterminate x over I.

Theorem: $\{I[x],+,\cdot\}$ is an integral domain.
<2.3.02>

Definition: A field is an integral domain in which every
<2.3.03> non-zero element has a unique multiplicative inverse. If we define $\{F,\oplus,\odot\}$ to be a finite field, then by the above $\{F[x],\oplus,\odot\}$ is an integral domain.

Definition: Let $p,a \in F[x]$; p is monic and $\deg(p) \geq 1$.
<2.3.04> Then by the division algorithm over $F[x]$, there exist unique $q,r \in F[x]$ such that $a = (q \odot p) \oplus r$ where $\deg(r) < \deg(p)$. Then define $a(\mathrm{mod}\ p) = r$.

Definition: Let $p \in F[x]$; p is monic and $\deg(p) \geq 1$.
<2.3.05> Define $F_1 = \{a \mid a \in F[x], \deg(a) < \deg(p)\}$. Two binary operations on F_1 are defined as follows

$$\overset{1}{\oplus} : F_1 \times F_1 \longrightarrow F_1, \quad a,b \in F_1 \Rightarrow a \overset{1}{\oplus} b = a \oplus b$$

$$\overset{1}{\odot} : F_1 \times F_1 \longrightarrow F_1, \quad a \overset{1}{\odot} b = (a \odot b)(\mathrm{mod}\ p)$$

Theorem: $\{F_1,\overset{1}{\oplus},\overset{1}{\odot}\}$ is a commutative ring with identity.
<2.3.06>

Proof: $F_1 \subset F[x]$. F_1 is closed, associative and commutative for $\overset{1}{\oplus}$ and $\overset{1}{\odot}$ and contains the additive inverse of each element in F_1. The distributive property follows from the fact that F_1 is closed under the operations $\oplus$.

that $F[x]$ is distributive with respects to $\oplus$, $\odot$ and that $(a \oplus b)(\text{mod } p) = a(\text{mod } p) \oplus b(\text{mod } p)$ for $a,b \in F_1$.

Definition: <2.3.07> $p \in F[x]$ is said to be irreducible if $\nexists$ $a,b \in F[x]$ such that $p = a \odot b$. p is said to be a prime polynomial (prime element or prime) in $F[x]$ if p is a monic irreducible polynomial in $F[x]$ and if $\deg(p) \geq 1$.

Theorem: <2.3.08> If p is a prime polynomial, $\{F_1, \overset{1}{\oplus}, \overset{1}{\odot}\}$ is a field.

Proof: Since p is prime there exist no $a,b \in F_1$ such that $a \odot b = p = 0 \ (\text{mod } p)$ and hence F_1 has no divisors of zero. Since F_1 is also commutative and has a unit, it is a field.

Definition: <2.3.09> Let F be a field and $F_1 \subset F[x]$ as defined in <2.3.05>. Define the function M by the following:

$$M : F[x] \longrightarrow F_1 \text{ where } a \in F[x] \Rightarrow aM = a(\text{mod } p)$$

Theorem: <2.3.10> M is a ring homomorphism from $F[x]$ onto F_1 or more concisely $M : F[x] \xrightarrow[\text{onto}]{H} F_1$.

Theorem: Let $\{R,\oplus,\odot\}$, $\{R_1,\overset{1}{\oplus},\overset{1}{\odot}\}$, $\{R_2,\overset{2}{\oplus},\overset{2}{\odot}\}$ be rings. Then
<2.3.20> $T_1 : R \xrightarrow{H} R_1$, $T_2 : R_1 \xrightarrow{H} R_2 \Rightarrow T = (T_1T_2) : R \xrightarrow{H} R_2$

Proof: Let $\bigcirc$ represent either of the operators $\oplus$ or $\odot$ and let $a,b \in R$. Then $(a \bigcirc b)T_1T_2 = (aT_1 \overset{1}{\bigcirc} bT_1)T_2 = aT_1T_2 \overset{2}{\bigcirc} bT_1T_2$ using the fact that T_1 and T_2 are homomorphisms and that $aT_1, bT_1 \in R_1$. Hence the composite function $T = (T_1T_2)$ is also a ring homomorphism.

2.4 The Modeled Domains

In this section we proceed to define a sequence of polynomial rings over an integral domain. In polynomial manipulation on a computer the polynomials with which one is working are normally in these rings and therefore we call them the "modeled domains".

Definition: The rings I_i, $i \geq 0$ are defined as follows:
<2.4.01> I_0 is the ring of all integers, an integral domain with respect to the operations $(+,\circ)$. For $i > 0$, let I_{i-1} be a ring with respect to the operations $(+,\circ)$. Define $I_i = I_{i-1}[x_i]$. By theorem <2.2.10> $\{I_i,+,\circ\}$ is also a ring. The retention of the operators $(+,\circ)$ is justified by the conventions made in <2.2>.

Lemma: I_i is an integral domain.
<2.4.02>

Proof: I_0 is an integral domain and by <2.3.02> and by induction on i, so is I_i for $0 \leq i$.

Lemma: $I_i \subseteq I_j$, $0 \leq i \leq j$
<2.4.03>

Proof: Strictly speaking, the statement is not true since I_{j+1} is a vector space over I_j. However, an embedding isomorphism can be defined which maps $a \in I_j$ into $(a,0,0,\ldots) = ax_{j+1}^0 \in I_{j+1}$. The normal convention is to make no distinction between I_j and its embedding in I_{j+1}, a convention we can also adopt since no confusion will result. With this in mind, the lemma holds trivially by induction on $h = j-i$.

Definition: Let $a \in I_i$; $a = \sum_{k=0}^{m} a_k x_i^k$, $a_m \neq 0$ for $0 < i$.
<2.4.04>

$$\deg_j(a) = \begin{cases} -\infty & a = 0 \\ 0 & 0 = j = i \\ m & 0 < j = i \\ \max(\deg_j(a_0), \ldots, \deg_j(a_m)) & 0 \leq j < i \\ 0 & 0 < i < j \end{cases}$$

Lemma: $a \in I_i \Rightarrow \deg_j(a) \leq 0$, $0 \leq i < j$.
<2.4.05>

Proof: $I_i \subseteq I_j$ and by the discussion in <2.4.03>.

<u>Definition</u>: Define the function $D^{-1}_{i,j} : I_i \longrightarrow I'_i$ as follows: Let $a \in I_i$; if $i > 0$, let $a = \sum_{k=0}^{m} a_k x_i^k$, $a_k \in I_{i-1}$.
<2.4.06>

$$aD^{-1}_{i,j} = \begin{cases} a & 0 \leq i \leq j \\ \sum_{k=0}^{m} (a_k D^{-1}_{i-1,j}) & 0 \leq j < i \end{cases}$$

where $I'_i = \{b \mid b = aD^{-1}_{i,j},\ a \in I_i\}$

<u>Lemma</u>: $I'_i \subseteq I_j$
<2.4.07>

Proof: Case 1: $0 \leq i \leq j$: by <2.4.03>

Case 2: $0 \leq j < i$: Let $h = i-j$. Assume that for some $h > 0$, $I'_i \subseteq I_j$. Let $a \in I_{i+1}$, $a = \sum_{k=0}^{m} a_k x_{i+1}^k$, $a_k \in I_i$. Then $aD^{-1}_{i+1,j} = \sum_{k=0}^{m} (a_k D^{-1}_{i,j}) \in I_j$ since $a_k D^{-1}_{i,j} \in I_j$ by the inductive hypothesis and $\{I_j, +, \cdot\}$ is an integral domain. For $h = 1$, $a_k D^{-1}_{i,j} = a_k D^{-1}_{j,j} = a_k$. Hence $aD^{-1}_{j+1,j} \in I_j$. The lemma holds by induction on h.

<u>Lemma</u>: $D^{-1}_{i,j} : I_i \xrightarrow{H} I_j$
<2.4.08>

Proof: Case 1: $0 \leq i \leq j$: $D^{-1}_{i,j}$ is the identity mapping.

Case 2: $0 \leq j \leq i$: Assume lemma true for $h = i - j \geq 0$. Let $a, b \in I_{i+1}$: $a = \sum_{k=0}^{K} a_k x_{i+1}^k$,

$b = \sum_{m=0}^{M} b_m x_{i+1}^m$, $N = \max(K,M)$. $aD_{i+1,j}^{-1} + bD_{i+1,j}^{-1} =$

$\sum_{n=0}^{N} (a_n D_{i,j}^{-1} + b_n D_{i,j}^{-1}) = \sum_{n=0}^{N} (a_n + b_n) D_{i,j}^{-1} = (a + b) D_{i+1,j}^{-1}$

since $D_{i,j}^{-1}$ is a homomorphism by the inductive hypothesis.

$$(aD_{i+1,j}^{-1}) \circ (bD_{i+1,j}^{-1}) = \sum_{n=0}^{K+M} \Big(\sum_{k+m=n} ((a_k D_{i,j}^{-1}) \circ (b_m D_{i,j}^{-1})) \Big)$$

$$= \sum_{n=0}^{K+M} \Big(\sum_{k+m=n} (a_k \circ b_m) \Big) D_{i,j}^{-1}$$

$$= (a \circ b) D_{i+1,j}^{-1}$$

For $h = 0$ the lemma is true by case 1. By induction on h the lemma is also true for case 2.

2.5 The Model Domains

Starting with a finite field of prime order we define sequences of finite fields and integral domains on adjunctions of the prime field. Since the modeling process will involve the mapping of polynomials in the modeled domains into these finite fields and integral domains, we refer to them as the 'model domains'. They will be denoted by F_j and J_j^α as defined in the following development.

<u>Definition</u>: $F_0 = \{0,1,2,\ldots,p_0-1\}$ where p_0 is a prime integer in I_0. <2.5.01>

Definition: Let $\oplus$ and $\odot$ be represented by $\bigcirc$. Then define
<2.5.02>

$\overset{-1}{\bigcirc} : I_0 \times I_0 \longrightarrow I_0$ where $a,b \in I_0 \Rightarrow a \overset{-1}{\bigcirc} b = a \bigcirc b$.
More specifically $a \overset{-1}{\oplus} b = a + b$;
$a \overset{-1}{\odot} b = a \cdot b$.

$\overset{0}{\bigcirc} : F_0 \times F_0 \longrightarrow F_0$ where $a,b \in I_0 \Rightarrow a \overset{0}{\bigcirc} b =$
$(a \bigcirc b) \pmod{p_0}$.

Lemma: $\{F_0, \overset{0}{\oplus}, \overset{0}{\odot}\}$ is a field.
<2.5.03>

Definition: A function M_0 mapping I_0 into I_0 is defined by $M_0 : I_0 \longrightarrow I_{p_0}$ where
<2.5.04>
$aM_0 = a \pmod{p_0}$ for $a \in I_0$ and
$I_{p_0} = \{b \mid b = aM_0, a \in I_0\}$ and p_0 is a prime integer.

Theorem: $M_0 : I_0 \xrightarrow[\text{onto}]{H} F_0$
<2.5.05>

Proof: Given in most texts with a section on number theory.

Definition: Define E_{j-1} to be a finite field for $0 < j$ with respect to the operations $\overset{j-1}{\oplus}, \overset{j-1}{\odot}$. Let
<2.5.07>
p_j be a prime polynomial in $E_{j-1}[x_j]$. Define
$d_j = \deg_j(p_j)$ to be the degree of p_j in the indeterminate x_j.

Definition: $F_j = \{a \mid a \in E_{j-1}[x_j],\ \deg_j(a) < d_j\}$ for $0 < j$.
<2.5.08>

Definition: The operation $\overset{j}{\circ}$, representing $\overset{j}{\oplus}$ or $\overset{j}{\odot}$ is
<2.5.09> defined as follows for $0 < j$:

$$\overset{j}{\circ} : F_j \times F_j \longrightarrow F_j;\ a,b \in F_j \Rightarrow a \overset{j}{\circ} b = (a \overset{j-1}{\circ} b) \pmod{p_j}$$

Theorem: $\{F_j, \overset{j}{\oplus}, \overset{j}{\odot}\}$ is a field for $0 < j$.
<2.5.10>

Proof: By theorem <2.3.08>.

Definition: The fields E_{j-1} in definition <2.5.07> were
<2.5.11> unspecified and not necessarily related. We now define $E_j = F_j$ for $0 < j$. Consequently $p_j \in F_{j-1}[x_j]$ and the operators can be seen to be consistent.

Theorem: $\{F_j[x_{j+1}], \overset{j}{\oplus}, \overset{j}{\odot}\}$ is an integral domain.
<2.5.12>

Proof: By theorem <2.3.02>.

Definition: A function M_j, $0 < j$, associated with the
<2.5.13> prime polynomial $p_j \in F_{j-1}[x_j]$ is defined as follows: $M_j : F_{j-1}[x_j] \longrightarrow I_{p_j}$ where $aM_j = a \pmod{p_j}$ for $a \in F_{j-1}[x_j]$. $I_{p_j} = \{b \mid b = aM_j;\ a \in F_{j-1}[x_j]\}$.

Theorem: $I_{p_j} = F_j$, $0 < j$.
<2.5.14>

Proof: Let $a \in F_{j-1}[x_j]$. By definition $\deg_j(a(\text{mod } p_j)) < d_j$. Therefore $\deg_j(aM_j) < d_j$ and $aM_j \in F_j$. As a ranges over $F_{j-1}[x_j]$, all of I_{p_j} is mapped out. Hence $I_{p_j} \subseteq F_j$. Let $b \in F_j$. Then $\deg_j(b) < d_j$. Therefore $bM_j = b(\text{mod } p_j) = b \in I_{p_j}$ and $F_j \subseteq I_{p_j}$.

Theorem: $M_j : F_{j-1}[x_j] \xrightarrow[\text{onto}]{H} F_j$, $0 < j$
<2.5.15>

Proof: By theorem <2.3.10>.

Lemma: $F_j \subseteq F_{j-1}[x_j]$, $0 < j$
<2.5.17>

Proof: By definition of E_{j-1}, F_j and <2.5.11>.

Theorem: $F_i \subseteq F_j$, $0 \leq i \leq j$
<2.5.18>

Proof: Let $h = j - i$. For $h = 0$, $F_i = F_j \subseteq F_j$. Assume that for some $h \geq 0$, $F_i \subseteq F_j$. Then $F_{j+1} \subseteq F_j[x_{j+1}]$ by <2.5.17> and F_j is embedded in both $F_j[x_{j+1}]$ and F_{j+1} since $d_j \geq 1$. Hence $F_j \subseteq F_{j+1}$ and consequently the theorem holds by induction on h.

Corollary: $F_i \subseteq F_j[x_{j+1}]$, $0 \leq i \leq j$
<2.5.19>

Proof: By <2.5.18> and <2.5.17>.

Theorem: $F_i \subseteq F_j \subseteq F_{j-1}[x_j] \subseteq I_j,\ 0 \leq i < j$
<2.5.20>

Proof: The first two relations hold by <2.5.18> and <2.5.19>. By definition $F_0 \subseteq I_0$, implying $F_0[x_1] \subseteq I_0[x_1] = I_1$. Assume that $F_{j-1}[x_j] \subseteq I_j$ for some $j \geq 1$. Then $F_j \subseteq F_{j-1}[x_j]$ implies $F_j \subseteq I_j$ and $F_j[x_{j+1}] \subseteq I_j[x_{j+1}] = I_{j+1}$. By induction on j, $F_{j-1}[x_j] \subseteq I_j$ for $0 < j$.

Lemma: $a \in F_i \Rightarrow \deg_j(a) \leq 0,\ 0 \leq i < j$
<2.5.21>

Proof: $\forall\ b \in F_{j-1},\ \deg_j(b) \leq 0$ since the embedding of F_{j-1} into F_j maps all elements in F_{j-1} into polynomials in x_j in F_j which are of degree 0. The proof is completed by <2.5.20>.

Theorem: $a \in F_j \Rightarrow aM_j = a$
<2.5.22>

Proof: $a \in F_j \Rightarrow a \in F_{j-1}[x_j]$ by <2.5.20> and $\deg_j(a) < d_j$. Therefore $aM_j = a \pmod{p_j} = a$.

Theorem: $a,b \in F_i \Rightarrow a \overset{j}{\bigcirc} b = a \overset{i}{\bigcirc} b,\ 0 \leq i \leq j$
<2.5.23>

Proof: Let $h = j - i$. For $h = 0$, the theorem is true

trivially. Assume that for some $h \geq 0$, $a \overset{j}{\circ} b = a \overset{i}{\circ} b$, for $a,b \in F_i$. $a,b \in F_j \subseteq F_{j+1}$ by <2.5.20> and $\deg_{j+1}(a) \leq 0$, $\deg_{j+1}(b) \leq 0$. Therefore $a \overset{j+1}{\circ} b = (a \overset{j}{\circ} b) \bmod p_{j+1} = a \overset{j}{\circ} b$ since $a \overset{j}{\circ} b \in F_j$ and $\deg_{j+1}(a \overset{j}{\circ} b) \leq 0$. By induction on h, the lemma holds.

Corollary: $a \in F_i \Rightarrow aM_j = a$, $0 \leq i \leq j$
<2.5.24>

Proof: By <2.5.20> and <2.5.22>.

Definition: The sets J_j^α are defined as follows:
<2.5.50>

$$J_j^\alpha = \begin{cases} F_j & \text{for } 0 \leq j \leq \alpha \\ J_{j-1}^\alpha[x_j] & \text{for } 0 \leq \alpha < j \end{cases}$$

Lemma: $F_j \subseteq J_j^\alpha \subseteq I_j$
<2.5.51>

Proof: Case 1: $0 \leq j \leq \alpha$ by <2.5.20>

Case 2: $0 \leq \alpha < j$: Let $h = j - \alpha$. For $h = 0$, $F_j = J_j^\alpha$ and $F_j \subseteq J_j^\alpha \subseteq I_j$. Assume that for some $h \geq 0$, $F_j \subseteq J_j^\alpha \subseteq I_j$. Let $a \in F_{j+1}$. Therefore $a \in F_j[x_{j+1}] \subseteq J_j^\alpha[x_{j+1}] = J_{j+1}^\alpha$ by the inductive hypothesis. Hence $F_{j+1} \subseteq J_{j+1}^\alpha$. $J_j^\alpha \subseteq I_j \Rightarrow J_{j+1}^\alpha = J_j^\alpha[x_{j+1}] \subseteq I_j[x_{j+1}] = I_{j+1}$. The lemma holds by induction on h.

Lemma: $F_{j-1}[x_j] \subseteq J_j^\alpha$, $0 \leq \alpha < j$
<2.5.52>

Proof: $F_{j-1} \subseteq J_{j-1}^\alpha$ by <2.5.51> and hence
$F_{j-1}[x_j] \subseteq J_{j-1}^\alpha[x_j] = J_j^\alpha$

Lemma: $J_i^\alpha \subseteq J_j^\alpha$, $0 \leq i \leq j$
<2.5.53>

Proof: Case 1: $0 \leq i \leq j \leq \alpha$: by <2.5.20>, <2.5.18>.

Case 2: $0 \leq i \leq \alpha < j$: $J_i^\alpha = F_i \subseteq F_{j-1}[x_j] \subseteq J_j^\alpha$ by <2.5.52>.

Case 3: $0 \leq \alpha < i \leq j$: Let $h = j - i$. For $h = 0$, $J_j^\alpha \subseteq J_j^\alpha$. Assume that for some $h \geq 0$, $J_i^\alpha \subseteq J_j^\alpha$ and $a \in J_i^\alpha$. Then $a \in J_j^\alpha \subseteq J_j^\alpha[x_{j+1}] = J_{j+1}^\alpha$. The case holds by induction on h.

Theorem: $\{J_j^\alpha, \overset{\alpha}{\oplus}, \overset{\alpha}{\odot}\}$ is an integral domain.
<2.5.54>

Proof: First it must be established that $(\overset{\alpha}{\oplus}, \overset{\alpha}{\odot})$ are valid binary operators on $J_j^\alpha \times J_j^\alpha$.

Case 1: $0 \leq j \leq \alpha$: $J_j^\alpha = F_j$ and $a, b \in F_j \Rightarrow a \overset{\alpha}{O} b = a \overset{j}{O} b$ by <2.5.23>. Consequently $\{J_j^\alpha, \overset{\alpha}{\oplus}, \overset{\alpha}{\odot}\}$ is a field and hence an integral domain.

Case 2: $0 \leq \alpha < j$: Let $h = j - \alpha$. For $h = 1$, $\{J_{\alpha+1}^\alpha, \overset{\alpha}{\oplus}, \overset{\alpha}{\odot}\}$ is an integral domain by <2.3.02>. Since $J_{j+1}^\alpha = J_j^\alpha[x_{j+1}]$, $\{J_{\alpha+h}^\alpha, \overset{\alpha}{\oplus}, \overset{\alpha}{\odot}\}$ is an integral domain by <2.3.02> and induction on h.

2.6 Further Conventions on Notation

In chapters 3 and 4 it will be convenient to have available a set of conventions about functional notation which will help to reduce the size of expressions and equations involving functions. We therefore define the following:

<u>Definition</u>: <2.6.01> Let A be a set $(A)^1 = A$; $A^{n+1} = (A)^n \times A$.
$(A)^n = \{a \mid a = (a_0, a_1, a_2, \ldots, a_{n-1}),\ a_k \in A\}$.

<u>Definition</u>: <2.6.02> The component extraction operator K_k is defined by $K_k : (A)^n \longrightarrow A$;
$aK_k = a_k$ where $a = (a_0, \ldots, a_k, \ldots a_{n-1})$.

<u>Definition</u>: <2.6.03> The function distribution operator is defined by $\theta : (A)^n \times F \longrightarrow (A \times F)^n$ where
$F = \{f \mid f : A \longrightarrow B\}$. $a \in (A)^n$, $f \in F \Rightarrow (a,f)\theta = (a_0 f, a_1 f, \ldots, a_{n-1} f)$.

<u>Definition</u>: <2.6.04> Let $f : A \longrightarrow B$, $a \in A$. Then define
$a(f)^n = a$ for $n \leq 0$; $a(f)^n = a(f)^{n-1} f$
for $n > 0$.

<u>Convention</u>: <2.6.05> It will sometimes be convenient to treat a binary operator as a unary operator modified

by the second in the pair of operands. Let $f : A \times B \longrightarrow C$, $a \in A$, $b \in B$. Define $af^{b} = (a,b)f$. The following are some examples:

$$(a_0,a_1,a_2) = a \in (A)^3 \Rightarrow a(\overset{f}{\theta})^4 K_2 = a_2ffff$$
$$a(\overset{f}{\theta})^2 = (a_0ff,a_1ff,a_2ff)$$

<u>Definitions</u>: <2.6.06>

$J^{\alpha} = \{J_i^{\alpha} \mid 0 \leq i\}$

$J = \{J^{\alpha} \mid -1 \leq \alpha\}$ (J-domains)

$I = \{I_i \mid 0 \leq i\} = J^{-1}$ (modeled domains)

$F = \{F_i \mid 0 \leq i\}$ (F-domains)

The sequence $(p_0,p_1,p_2,\ldots)$ of <2.5.07> will sometimes be referred to as the "prime context sequence".

<u>Definition</u>: <2.6.07> $U = \{Z_0^+,\infty\}$. The symbol ∞ has the following properties: $\forall\, a \in Z_0^+$, $\infty + a = \infty$; $\infty - a = \infty$; $a < \infty$.

CHAPTER III THE RECURSIVE MODELING FUNCTIONS

3.1 Introduction

At this point we have available a sequence of modeled domains $(I_0, I_1, \ldots, I_i, \ldots)$ which are integral domains with respect to the operations $(+, \cdot)$. Based on a prime integer p_0 in I_0 we have defined a sequence of F domains $(F_0, F_1, \ldots, F_j, \ldots)$ each of which is a finite field generated by the sequence of prime elements $(p_0, p_1, \ldots, p_j, \ldots)$ where p_j is a prime polynomial in $F_{j-1}[x_j]$ for $0 < j$. The ring operations on the sequence of F domains are represented by the operator sequence $((\oplus_0, \odot_0), (\oplus_1, \odot_1), \ldots, (\oplus_j, \odot_j), \ldots)$. Based on the F domains sets of sequences of J domains were generated one of which is represented by $(F_0, F_1, \ldots, F_{\alpha-1}, F_\alpha, J^\alpha_{\alpha+1}, \ldots, J^\alpha_j, \ldots)$ where F_0 through F_α are finite fields as in the F domains and $J^\alpha_{\alpha+1}, J^\alpha_{\alpha+2}, \ldots$ are integral domains formed by successive adjunctions on F_α. The corresponding operator sequence is then

$$((\oplus_0, \odot_0), (\oplus_1, \odot_1), \ldots, (\oplus_{\alpha-1}, \odot_{\alpha-1}), (\oplus_\alpha, \odot_\alpha), (\oplus_\alpha, \odot_\alpha), \ldots)$$

The object of this chapter is to define sets of functions which map an element from any of the modeled domains into any of the F or J domains and which in addition are homomorphisms.

3.2 The C Modeling Functions

<3.2.01> **Definition:** The function $C_{i,j} : I_i \longrightarrow I^{\infty}_{i,j}$ is defined by the following: $I^{\infty}_{i,j} = \{b \mid b = aC_{i,j},\ a \in I_i\}$.

Let $a \in I_i$. Then if $i > 0$, we assume a has degree m $a = \sum_{k=0}^{m} a_k x_i^k$ where $a_k \in I_{i-1}$. Define the auxiliary function $C'_{i,j} : I_i \longrightarrow I'_{i,j}$ where $I'_{i,j} = \{c \mid c = aC'_{i,j},\ a \in I_i\}$ and the image of a is

$$aC'_{i,j} = \begin{cases} a & \text{for } 0 = i = j \\ \sum_{k=0}^{m} (a_k C_{j-1,j-1}) x_j^k & \text{for } 0 < i = j \\ \sum_{k=0}^{m} \bigoplus^{j-1} (a_k C'_{i-1,j}) & \text{for } 0 \leq j < i \\ aC_{i,j-1} & \text{for } 0 \leq i < j \end{cases}$$

Then define $aC_{i,j} = aC'_{i,j} M_j$

where $M_0 : I_0 \longrightarrow F_0$; $aM_0 = a \pmod{p_0}$

$M_j : F_{j-1}[x_j] \longrightarrow F_j$; $aM_j = a \pmod{p_j}$ $0 < j$

A necessary and sufficient condition that the above definition be valid is that $I'_{i,0} \subseteq I_0$ and $I'_{i,j} \subseteq F_{j-1}[x_j]$ for $0 < j$. This condition is shown to hold

in Theorem <3.3.16>. In addition it is shown that $I^{\infty}_{i,j} \subseteq F_j$ and that $C_{i,j}$ is a homomorphism from I_i into F_j.

3.3 The C Modeling Theorem Proofs

The purpose of this section is to prove the following two theorems:

$$I^{\uparrow}_{i,0} \subseteq I_0;\ I^{\uparrow}_{i,j} \subseteq F_{j-1}[x_j] \text{ for } 0 < j \quad \langle 3.3.16 \rangle$$

$$C_{i,j} : I_j \xrightarrow{H} F_j \quad \langle 3.3.25 \rangle$$

The above two results are the only ones required for further developments. If the reader is willing to accept their validity he may skip the rest of this section and go to section 3.4.

Lemma: $a \in I_j \Rightarrow aC^{\uparrow}_{i,j} = aC^{\uparrow}_{j,j},\ 0 \leq j \leq i$ <3.3.01>

Proof: $a \in I_j \Rightarrow a \in I_i$ by <2.4.03>. Let $h = i - j$. For $h = 0$, the lemma holds trivially. Assume that for some $h \geq 0$, $aC^{\uparrow}_{i,j} = aC^{\uparrow}_{j,j}$. $a \in I_i \Rightarrow a \in I_{i+1}$ and $\deg_{i+1}(a) = 0$. $aC^{\uparrow}_{i+1,j} = \sum_{k=0}^{0} {}^{j-1}_{+}(aC^{\uparrow}_{i,j}) = aC^{\uparrow}_{i,j} = aC^{\uparrow}_{j,j}$. By induction on h the lemma is true.

Lemma: $I^{\uparrow}_{0,0} = I_0;\ I^{\infty}_{0,0} = F_0$ <3.3.02>

Proof: $C^{\prime}_{0,0}$ is the identity mapping from I_0 onto I_0 and hence $I^{\prime}_{0,0} = I_0$. Let $a \in I_0$. Then $aC_{0,0} = (aC^{\prime}_{0,0})M_0 = aM_0 \in F_0$. Therefore $I^{\infty}_{0,0} \subseteq F_0$. Let $b \in F_0$. Then $b \in I_0$ by <2.5.18> and $bC_{0,0} = aM_0 = a$ by <2.5.24>. Therefore $F_0 \subseteq I^{\infty}_{0,0}$.

Lemma: $I^{\prime}_{j,j} \subseteq F_{j-1}[x_j]$, $I^{\infty}_{j,j} \subseteq F_j$ for $0 < j$
<3.3.03>

Proof: For $j = 1$, let $a \in I_j$; $a = \sum_{k=0}^{m} a_k x_1^k$; $a_k \in I_0$. $aC^{\prime}_{1,1} = \sum_{k=0}^{m} (a_k C_{0,0}) x_1^k \in F_0[x_1]$ since $a_k C_{0,0} \in F_0$ by <3.3.02>. Hence $I^{\prime}_{1,1} \subseteq F_0[x_1]$ since $I^{\prime}_{1,1}$ is mapped out completely as a ranges over I_1. Let $b \in I_1$. Then $bC^{\prime}_{1,1} \in F_0[x_1]$ and $(bC^{\prime}_{1,1})M_1 \in F_1$. But $bC_{1,1} = (bC^{\prime}_{1,1})M_1 \in I^{\infty}_{1,1}$ implying that $I^{\infty}_{1,1} \subseteq F_1$. Assume for some $j > 0$ that $I^{\prime}_{j,j} \subseteq F_{j-1}[x_j]$ and $I^{\infty}_{j,j} \subseteq F_j$. Let $a \in I_{j+1}$; $a = \sum_{k=0}^{m} a_k x_{j+1}^k$; $a_k \in I_j$. Then $aC^{\prime}_{j+1,j+1} = \sum_{k=0}^{m} (a_k C_{j,j}) x_{j+1}^k \in F_j[x_{j+1}]$ since $aC_{j,j} \in I^{\infty}_{j,j} \subseteq F_j$ by the inductive hypothesis. Therefore $I^{\prime}_{j+1,j+1} \subseteq F_j[x_{j+1}]$. $(aC^{\prime}_{j+1,j+1})M_{j+1} \in F_{j+1}$ and $aC_{j+1,j+1} = (aC^{\prime}_{j+1,j+1})M_j \in I^{\infty}_{j+1,j+1}$. Therefore $I^{\infty}_{j+1,j+1} \subseteq F_{j+1}$. By induction on j the lemma holds.

Lemma: $I^{\infty}_{j,j} \subseteq F_j$
<3.3.04>

Proof: A combination of <3.3.02> when $j = 0$ and <3.3.03> when $j \geq 0$.

Lemma: $C^{\circ}_{i,j} = C_{i,i}$, $0 \leq i < j$
<3.3.05>

Proof: Let $h = j - i$ for some $i \geq 0$. Let $a \in I_i$. Then for $h = 1$, $aC^{\circ}_{i,i+1} = aC_{i,i}$ and consequently $C^{\circ}_{i,i+1} = C_{i,i}$ since a can range over all elements in I_i. Assume that for some $h > 0$, $C^{\circ}_{i,j} = C_{i,i}$. Then $aC^{\circ}_{i,j+1} = aC_{i,j} = (aC^{\circ}_{i,j})M_j = (aC_{i,i})M_j$ by the inductive hypothesis. Since $aC_{i,i} \in F_i$ by <3.3.04> and $F_i \subseteq F_j$ by <2.5.18> we have $aC_{i,i} \in F_j$ and $(aC_{i,i})M_j = aC_{i,i}$ by <2.5.24>. Therefore $aC^{\circ}_{i,j+1} = aC_{i,i}$ and $C^{\circ}_{i,j+1} = C_{i,i}$. By induction on h, the lemma holds.

Lemma: $b \in F_j \Rightarrow bC_{j,j} = b$
<3.3.06>

Proof: $b \in F_j \Rightarrow b \in I_j$ by <2.5.20>. For $j = 0$, $b \in F_0$ and $bC_{0,0} = bM_0 = b$ by <2.5.24>. Suppose that for some $j \geq 0$, $b \in F_j \Rightarrow bC_{j,j} = b$. Then let $a \in F_{j+1}$: $a = \sum_{k=0}^{m} a_k x_{j+1}^k$; $m < \deg_{j+1}(p_{j+1})$; $a_k \in F_j$. Then $aC^{\circ}_{j+1,j+1} = \sum_{k=0}^{m} (a_k C_{j,j}) x_{j+1}^k = \sum_{k=0}^{m} a_k x_{j+1}^k$ by the inductive hypothesis. Therefore $aC^{\circ}_{j+1,j+1} \in F_j[x_{j+1}]$ and $aC_{j+1,j+1} = (aC^{\circ}_{j+1,j+1})M_{j+1} = \sum_{k=0}^{m} a_k x_{j+1}^k = a$ since

$m < \deg_{j+1}(p_{j+1})$. The lemma holds by induction on j.

Lemma: $F_j \subseteq I^{\infty}_{j,j}$
<3.3.07>

Proof: For $j = 0$, $F_0 = I^{\infty}_{0,0}$ by <3.3.02>. Assume that for some $j \geq 0$ $F_j \subseteq I^{\infty}_{j,j}$. Let $a \in F_{j+1}$; $a = \sum_{k=0}^{m} a_k x_{j+1}^k$; $a_k \in F_j$; $m < \deg_{j+1}(p_{j+1})$. Then
$aC'_{j+1,j+1} = \sum_{k=0}^{m} (a_k C_{j,j}) x_{j+1}^k \in F_j[x_{j+1}]$ by <3.3.03>.

$$aC_{j+1,j+1} = \left(\sum_{k=0}^{m} (a_k C_{j,j}) x_{j+1}^k\right) M_{j+1}$$
$$= \sum_{k=0}^{m} (a_k C_{j,j}) x_{j+1}^k \quad \text{since} \quad m < \deg_{j+1}(p_{j+1})$$
$$= \sum_{k=0}^{m} a_k x_{j+1}^k = a \quad \text{by <3.3.06>}$$

Therefore $F_{j+1} \subseteq I^{\infty}_{j+1,j+1}$. The lemma holds by induction on j.

Lemma: $F_{j-1}[x_j] \subseteq I'_{j,j}$, $0 < j$
<3.3.08>

Proof: For $j = 1$, let $a \in F_0[x_1]$; $a = \sum_{k=0}^{m} a_k x_1^k$; $a_k \in F_0$.
$a \in I_1$ by <2.5.20> and
$aC'_{1,1} = \sum_{k=0}^{m} (a_k C_{0,0}) x_1^k = \sum_{k=0}^{m} a_k x_1^k = a \in I'_{1,1}$ by <3.3.06>.
Therefore $F_0[x_1] \subseteq I'_{1,1}$. Suppose that for some $j \geq 1$, $F_{j-1}[x_j] \subseteq I'_{j,j}$. Let $a \in F_j[x_{j+1}]$; $a = \sum_{k=0}^{m} a_k x_{j+1}^k$; $a_k \in F_j$.

Since $a \in I_{j+1}$ by <2.5.20>,

$aC^{\wedge}_{j+1,j+1} = \sum_{k=0}^{m} (a_k C_{j,j}) x_{j+1}^k = \sum_{k=0}^{m} a_k x_{j+1}^k = a$ by <3.3.06>.

Therefore $a \in I^{\wedge}_{j+1,j+1}$ and $F_j[x_{j+1}] \subseteq I^{\wedge}_{j+1,j+1}$. The lemma holds by induction on j.

Lemma: $I^{\infty}_{j,j} = F_j$
<3.3.09>

Proof: by <3.3.07> and <3.3.04>.

Lemma: $I^{\wedge}_{j,j} = F_{j-1}[x_j]$, $0 < j$
<3.3.10>

Proof: by <3.3.03> and <3.3.08>.

Lemma: $I^{\wedge}_{i,j} = F_i$, $0 \leq i < j$
<3.3.11>

Proof: Let $a \in I_i$ for some $i \geq 0$. Then $aC^{\wedge}_{i,j} = aC_{i,i} \in F_i$ by <3.3.05> and <3.3.04>. Therefore $I^{\wedge}_{i,j} \subseteq F_i$. Let $b \in F_i$. Then $b \in I_i$ and $bC_{i,i} = b$ by <3.3.06>. $bC^{\wedge}_{i,j} = bC_{i,i} = b \in I^{\wedge}_{i,j}$. Therefore $F_i \subseteq I^{\wedge}_{i,j}$.

Lemma: $I^{\wedge}_{i,j} = F_{j-1}[x_j]$, $0 < j \leq i$.
<3.3.12>

Proof: Let $h = i - j$ for some fixed $j > 0$. For $h = 0$, $I^{\wedge}_{j,j} = F_{j-1}[x_j]$ by <3.3.10>. Suppose that for some $h \geq 0$, $I^{\wedge}_{i,j} = F_{j-1}[x_j]$. Then $b \in I_i \Rightarrow bC^{\wedge}_{i,j} \in F_{j-1}[x_j]$. Let

$a \in I_{i+1}$: $a = \sum_{k=0}^{m} a_k x_{i+1}^k$; $a_k \in I_i$. Then

$aC'_{i+1,j} = \sum_{k=0}^{m} \overset{j-1}{\oplus} (aC'_{i,j}) \in F_{j-1}[x_j]$ by the inductive hypothesis and by <2.5.12>. Therefore $I'_{i+1,j} \subseteq F_{j-1}[x_j]$. Let $b \in F_{j-1}[x_j]$; $b = \sum_{k=0}^{m} b_k x_j^k$; $b_k \in F_{j-1}$. But then $b \in I_j \subseteq I_{i+1}$ by <2.5.20>. Therefore

$bC'_{i+1,j} = bC'_{j,j} = \sum_{k=0}^{m} (b_k C_{j-1,j-1}) x_j^k = \sum_{k=0}^{m} b_k x_j^k = b$ by <3.3.01> and <3.3.06>. Therefore $b \in I'_{i+1,j}$ and $F_{j-1}[x_j] \subseteq I'_{i+1,j}$ implying that $F_{j-1}[x_j] \subseteq I'_{i+1,j}$. The lemma holds by induction on h.

Lemma: $I^{\infty}_{i,j} = F_i$, $0 \leq i \leq j$
<3.3.13>

Proof: Let $h = j - i$ for some $i \geq 0$.

Case 1: $h = 0$: The lemma holds by <3.3.04>.

Case 2: $h > 0$: Let $a \in I_i$. Then

$aC'_{i,j} = aC_{i,i} \in F_i$ by <3.3.05> and <3.3.04>.

$aC_{i,j} = (aC'_{i,j})M_j = (aC_{i,i})M_j = aC_{i,i}$ by <2.5.24>. Therefore $aC_{i,j} \in F_i$ and $I^{\infty}_{i,j} \subseteq F_i$. Let $b \in F_i$. $b \in I_i$ and $bC_{i,i} = b$ by <3.3.06>; $b \in F_j$ by <2.5.18>.

$bC_{i,j} = (bC'_{i,j})M_j = (bC_{i,i})M_j = bM_j = b$ by <2.5.24>. Therefore $b \in I^{\infty}_{i,j}$ and $F_i \subseteq I^{\infty}_{i,j}$. Hence $I^{\infty}_{i,j} = F_i$ for $h > 0$.

Lemma: $I'_{i,0} = I_0$
<3.3.14>

Proof: $I'_{0,0} = I_0$ by <3.3.02>. Let $a \in I_0 \subseteq I_i$.
$aC'_{i,0} = aC'_{0,0} = a \in I'_{i,0}$ by <3.3.01>. Therefore $I_0 \subseteq I'_{i,0}$.
Suppose that for some $i \geq 0$, $I'_{i,0} \subseteq I_0$. Let $a \in I_{i+1}$
$aC'_{i+1,0} = \sum_{k=0}^{m} \overset{-1}{\oplus} (a_k C'_{i,0}) = \sum_{k=0}^{m} (a_k C'_{i,0}) \in I_0$ by <2.5.02>
and the inductive hypothesis. By induction on i,
$I'_{i,0} \subseteq I_0$ for $0 \leq i$.

Lemma: $I^{\infty}_{i,j} = F_j$, $0 \leq j \leq i$
<3.3.15>

Proof: Case 1: $0 = j \leq i$: For $i = 0$, $I^{\infty}_{0,0} = F_0$ by <3.3.02>. Let $a \in I_i$. Then $aC'_{i,0} \in I_0$ by <3.3.14> and $aC_{i,0} = (aC'_{i,0})M_0 \in F_0$. Hence $I^{\infty}_{i,0} \subseteq F_0$.
Let $b \in F_0$. Then $b \in I_0 \subseteq I_i$ by <2.5.18> and <2.4.03>
$bC'_{i,0} = bC'_{0,0} = b$ by <3.3.01> and therefore
$bC_{i,0} = (bC'_{i,0})M_0 = bM_0 = b$. Consequently $b \in I^{\infty}_{i,0}$ and $F_0 \subseteq I^{\infty}_{i,0}$.

Case 2: $0 < j \leq i$: Let $h = i - j$ for some $j > 0$. For $h = 0$, $I^{\infty}_{j,j} = F_j$ by <3.3.09>. Suppose that for some $h \geq 0$, $I^{\infty}_{j,j} = F_j$. Let $a \in F_j$: $a = \sum_{k=0}^{m} a_k x_j^k$; $a_k \in F_{j-1}$; $m < \deg_j(p_j)$; $a \in F_j \subset I_j \subseteq I_i \subseteq I_{i+1}$.
$aC'_{i+1,j} = aC'_{j,j} = \sum_{k=0}^{m} (a_k C_{j-1,j-1}) x_j^k = \sum_{k=0}^{m} a_k x_j^k = a$ by <3.3.01> and <3.3.06>. Therefore $a \in F_j \subseteq F_{j-1}[x_j]$ and $aC'_{i+1,j} \in F_{j-1}[x_j]$. Therefore $aC_{i+1,j} = (aC'_{i+1,j})M_j = aM_j = a$ by <3.3.01> and <2.5.24>. Hence $a \in I^{\infty}_{i+1,j}$ and $F_j \subseteq I^{\infty}_{i+1,j}$.

By induction on h, $F_j \subseteq I^{\infty}_{i,j}$ for $0 < j \leq i$. Let $b \in I_i$. $bC^{\prime}_{i,j} \in F_{j-1}[x_j]$ by <3.3.12> and hence $bC_{i,j} = (bC^{\prime}_{i,j})M_j \in F_j$. Therefore $I^{\infty}_{i,j} \subseteq F_j$ for $0 < j \leq i$. Consequently $I^{\infty}_{i,j} = F_j$ for case 2.

Theorem: $(I^{\prime}_{i,0} = I_0)$ and $(I^{\prime}_{i,j} \subseteq F_{j-1}[x_j],\ 0 < j)$ <3.3.16>

Proof: Case 1: $0 = j \leq i$: by <3.3.14>

Case 2: $0 < j \leq i$: by <3.3.12>

Case 3: $0 < i < j$: $I^{\prime}_{i,j} = F_j \subseteq F_j \subseteq F_{j-1}[x_j]$ by <3.3.11> and <2.5.20>.

Theorem: $I^{\infty}_{i,j} \subseteq F_j$ <3.3.17>

Proof: Case 1: $0 \leq j \leq i$: $I^{\infty}_{i,j} = F_j \subseteq F_j$ by <3.3.15>

Case 2: $0 < i < j$: $I^{\infty}_{i,j} = F_i \subseteq F_j$ by <3.3.13>.

Lemma: $C_{i,j} = C_{i,i}$ for $0 \leq i \leq j$ <3.3.18>

Proof: Let $h = j - i$ for some fixed $i \geq 0$.

Case 1: $h = 0$: The lemma holds trivially.

Case 2: $h > 0$: Let $a \in I_i$.

$aC_{i,j} = (aC^{\prime}_{i,j})M_j = (aC_{i,i})M_j$. But $aC_{i,i} \in F_i$ by <3.3.09> and $F_i \subseteq F_j$ since $h = j - i > 0$. Hence $(aC_{i,i})M_j = aC_{i,i}$ by <2.5.24>. Therefore $aC_{i,j} = aC_{i,i}$ and $C_{i,j} = C_{i,i}$.

Lemma: $b \in I_j \Rightarrow bC_{i,j} = bC_{j,j}$, $0 \leq j \leq i$ <3.3.19>

Proof: For any $i \geq j \geq 0$, $b \in I_i$.

$$bC_{i,j} = (bC'_{i,j})M_j = (bC'_{j,j})M_j \text{ by } \langle 3.3.16\rangle \text{ and } \langle 3.3.01\rangle$$
$$= bC_{j,j}$$

Theorem: $C_{j,j} : I_j \xrightarrow[\text{onto}]{H} F_j$ <3.3.20>

Proof: Since $I^{\infty}_{j,j} = F_j$ by <3.3.09>, we need only show that for $a,b \in I_i$, $aC_{j,j} \overset{j}{\oplus} bC_{j,j} = (a + b)C_{j,j}$ and $aC_{j,j} \overset{j}{\odot} bC_{j,j} = (a \circ b)C_{j,j}$

For $j = 0$, $C_0 = M_0 : I_0 \xrightarrow[\text{onto}]{H} F_0$ by <2.5.05>. Suppose that for $j \geq 0$, $C_{j,j} : I_j \xrightarrow{H} F_j$. Let $a \in I_{j+1}$: $a = \sum_{k=0}^{K} a_k x^k_{j+1}$; $a_k \in I_j$ and $b \in I_{j+1}$: $b = \sum_{m=0}^{M} b_m x^m_{j+1}$; $b_m \in I_j$. Define $N = \max(K,M)$. Then

$$a + b = \sum_{n=0}^{N} (a_n + b_n)x^n_{j+1}; \quad a \circ b = \sum_{n=0}^{K+M} \Big(\sum_{k+m=n} (a_k \circ b_m)\Big)x^n_{j+1}$$

$$aC_{j+1,j+1} \overset{j+1}{\oplus} bC_{j+1,j+1}$$
$$= \Big(\sum_{k=0}^{K} (a_k C_{j,j})x^k_{j+1}\Big)M_{j+1} \overset{j+1}{\oplus} \Big(\sum_{m=0}^{M} (b_m C_{j,j})x^m_{j+1}\Big)M_{j+1}$$
$$= \Big(\sum_{k=0}^{K} \overset{j}{\oplus} (a_k C_{j,j})x^k_{j+1}\Big)M_{j+1} \overset{j+1}{\oplus} \Big(\sum_{m=0}^{M} \overset{j}{\oplus} (b_m C_{j,j})x^m_{j+1}\Big)M_{j+1} \text{ by } \langle 2.2.30\rangle$$
$$= \Big(\sum_{k=0}^{K} \overset{j}{\oplus} (a_k C_{j,j})x^k_{j+1} \overset{j}{\oplus} \sum_{m=0}^{M} \overset{j}{\oplus} (b_m C_{j,j})x^m_{j+1}\Big)M_{j+1} \text{ by } \langle 3.3.17\rangle, \langle 2.5.15\rangle$$

$$= \left(\sum_{n=0}^{N} \overset{j}{\oplus} (a_n C_{j,j} \overset{j}{\oplus} b_n C_{j,j}) x_{j+1}^n\right) M_{j+1} \quad \text{by } \langle 2.5.10 \rangle$$

$$= \left(\sum_{n=0}^{N} \overset{j}{\oplus} ([a_n + b_n] C_{j,j}) x_{j+1}^n\right) M_{j+1} \quad \text{by the inductive hypothesis}$$

$$= (a + b) C_{j+1,j+1}$$

$$aC_{j+1,j+1} \overset{j+1}{\odot} bC_{j+1,j+1}$$

$$= \left(\sum_{k=0}^{N} \overset{j}{\oplus} (a_k C_{j,j}) x_{j+1}^k\right) M_{j+1} \overset{j+1}{\odot} \left(\sum_{m=0}^{M} \overset{j}{\oplus} (b_m C_{j,j}) x_{j+1}^m\right) M_{j+1}$$

$$= \left(\sum_{n=0}^{K+M} \overset{j}{\oplus} \left(\sum_{k+m=n} \overset{j}{\oplus} (a_k C_{j,j} \overset{j}{\odot} b_m C_{j,j})\right) x_{j+1}^n\right) M_{j+1} \quad \text{by } \langle 3.3.17 \rangle, \langle 2.5.15 \rangle \text{ and } \langle 2.5.10 \rangle$$

$$= \left(\sum_{n=0}^{K+M} \overset{j}{\oplus} \left(\sum_{k+m=n} \overset{j}{\oplus} ([a_k \circ b_m] C_{j,j})\right) x_{j+1}^n\right) M_{j+1} \quad \text{by the inductive hypothesis}$$

$$= \left(\sum_{n=0}^{K+M} \overset{j}{\oplus} \left(\left[\sum_{k+m=n} (a_k \circ b_m)\right] C_{j,j}\right) x_{j+1}^n\right) M_{j+1} \quad \text{again by the inductive hypothesis}$$

$$= (a \circ b) C_{j+1,j+1}$$

Therefore $C_{j+1,j+1} : I_{j+1} \xrightarrow{H} F_{j+1}$. By induction on j, the theorem holds.

<u>Corollary</u>: $C_{i,j} : I_i \xrightarrow{H} F_j$, $0 \leq i \leq j$ $\langle 3.3.21 \rangle$

Proof: For $0 \leq i \leq j$, $C_{i,j} = C_{i,i}$ by $\langle 3.3.18 \rangle$. Therefore $C_{i,j} : I_i \xrightarrow{H} F_i \subseteq F_j$.

Theorem: $C'_{i,0} : I_i \xrightarrow{H} I_0$
<3.3.22>

Proof: For $i = 0$, $C'_{0,0}$ is the identity mapping and therefore is a homomorphism. For $i > 0$, let $a,b \in I_{i+1}$:
$a = \sum_{k=0}^{K} a_k x_{i+1}^k$; $b = \sum_{k=0}^{M} b_k x_{i+1}^k$; $N = \max(K,M)$; $a_k, b_k \in I_i$.
Assume that for some $i \geq 0$, $C'_{i,0} : I_i \xrightarrow{H} I'_{i,0}$

$$aC'_{i+1,0} \overset{-1}{\oplus} bC'_{i+1,0}$$

$$= \sum_{k=0}^{K} \overset{-1}{\oplus} (a_k C'_{i,0}) \overset{-1}{\oplus} \sum_{m=0}^{M} \overset{-1}{\oplus} (b_m C'_{i,0}) \quad \text{by <2.5.02>}$$

$$= \sum_{n=0}^{N} \overset{-1}{\oplus} (a_n C'_{i,0} \overset{-1}{\oplus} b_n C'_{i,0}) \quad \text{by <2.4.02>}$$

$$= \sum_{n=0}^{N} \overset{-1}{\oplus} ([a_n + b_n] C'_{i,0}) \quad \text{by the inductive hypothesis}$$

$$= (a + b)C'_{i+1,0}$$

Similarly $aC'_{i+1,0} \overset{-1}{\odot} bC'_{i+1,0} = (a \circ b)C'_{i+1,0}$. By induction on i, the theorem holds.

Theorem: $C'_{i,j} : I_i \xrightarrow[\text{onto}]{H} F_{j-1}[x_j]$, $0 < j \leq i$
<3.3.23>

Proof: $C'_{i,j} : I_i \xrightarrow[\text{onto}]{} F_{j-1}[x_j]$ by <3.3.12>. Let $h = i - j$ for some $j > 0$. For $h = 0$, let $a \in I_j$; $a = \sum_{k=0}^{K} a_k x_j^k$; $a_k \in I_{j-1}$ and $b \in I_j$, $b = \sum_{m=0}^{M} b_m x_j^m$, $b_m \in I_{j-1}$.

Define $N = \max(K,M)$

$$aC^{\uparrow}_{j,j} \overset{j-1}{\oplus} bC^{\uparrow}_{j,j}$$

$$= \sum_{k=0}^{K} \overset{j-1}{\oplus} (a_k C_{j-1,j-1}) x_j^k \overset{j-1}{\oplus} \sum_{m=0}^{M} \overset{j-1}{\oplus} (b_m C_{j-1,j-1}) x_j^m$$

$$= \sum_{n=0}^{N} \overset{j-1}{\oplus} (a_n C_{j-1,j-1} \overset{j-1}{\oplus} b_n C_{j-1,j-1}) x_j^n \quad \text{by } \langle 2.5.12 \rangle$$

$$= \sum_{n=0}^{N} \overset{j-1}{\oplus} ([a_n + b_n] C_{j-1,j-1}) x_j^n \quad \text{by } \langle 3.3.20 \rangle$$

$$= (a + b) C^{\uparrow}_{j,j}$$

Similarly $aC^{\uparrow}_{j,j} \overset{j-1}{\odot} bC^{\uparrow}_{j,j} = (a \circ b) C^{\uparrow}_{j,j}$. Assume that for some $h = i - j \geq 0$, $C^{\uparrow}_{i,j} : I_i \xrightarrow{H} F_{j-1}[x_j]$. Let $a \in I_{i+1}$; $a = \sum_{k=0}^{K} a_k x_{i+1}^k$; $a_k \in I_i$ and $b \in I_{i+1}$; $b = \sum_{m=0}^{M} b_m x_{i+1}^m$; $b_m \in I_i$. Define $N = \max(K,M)$

$$aC^{\uparrow}_{i+1,j} \overset{j-1}{\oplus} bC^{\uparrow}_{i+1,j}$$

$$= \sum_{k=0}^{K} \overset{j-1}{\oplus} (a_k C^{\uparrow}_{i,j}) \overset{j-1}{\oplus} \sum_{m=0}^{M} \overset{j-1}{\oplus} (b_m C^{\uparrow}_{i,j})$$

$$= \sum_{n=0}^{N} \overset{j-1}{\oplus} (a_n C^{\uparrow}_{i,j} \overset{j-1}{\oplus} b_n C^{\uparrow}_{i,j}) \quad \text{by } \langle 3.3.12 \rangle, \langle 2.5.12 \rangle$$

$$= \sum_{n=0}^{N} \overset{j-1}{\oplus} ([a_n + b_n] C^{\uparrow}_{i,j}) \quad \text{by the inductive hypothesis}$$

$$= (a + b) C^{\uparrow}_{i+1,j}$$

Similarly $aC'_{i+1,j} \overset{j-1}{\circledcirc} bC'_{i+1,j} = (a \cdot b)C'_{i+1,j}$. Therefore the lemma holds by induction on h.

Corollary: $C_{i,j} : I_i \xrightarrow{H} F_j$, $0 \leq j \leq i$ <3.3.24>

Proof: Case 1: $0 = j \leq i$

$C'_{i,0} : I_i \xrightarrow{H} I_0$; $M_0 : I_0 \xrightarrow{H} F_0$ by <3.3.22>, <2.5.05>.

Hence $C_{i,j} = C'_{i,0}M_0 : I_i \xrightarrow{H} F_0$ by <2.3.20>.

Case 2: $0 < j \leq i$

$C'_{i,j} : I_i \xrightarrow{H} F_{j-1}[x_j]$; $M_j : F_{j-1}[x_j] \xrightarrow{H} F_j$ by <3.3.23>, <2.5.15>. Hence $C_{i,j} = C'_{i,j}M_j : I_i \xrightarrow{H} F_j$ by <2.3.20>.

Corollary: $C_{i,j} : I_i \xrightarrow{H} F_j$ <3.3.25>

Proof: Case 1: $0 < i < j$: by <3.3.21>.

Case 2: $0 \leq j \leq i$: by <3.3.24>.

3.4 The D Modeling Functions

The F-models as defined by the C modeling functions are useful in themselves, but they have the disadvantage of destroying the degree information in polynomials. Consequently we define another function from the modeled domains into the J domains in such a way that the degree information of selected indeterminates is preserved, with the additional requirement that the functions be homomorphisms. It will be shown that this is accomplished with the D modeling functions.

Definition: Define the function $D^{\alpha}_{i,j} : I_i \longrightarrow I^{\alpha}_{i,j}$ where
<3.4.01> $i,j,\alpha \in Z^{+}_{0}$, $I^{\alpha}_{i,j} = \{b \mid b = aD^{\alpha}_{i,j},\ a \in I_i\}$ as follows: Let $a \in I_i$. If $0 < i$, $a = \sum_{k=0}^{m} a_k x_i^k$; $a_k \in I_{i-1}$.

$$aD^{\alpha}_{i,j} = \begin{cases} aC_{i,j} & \text{for } 0 \le i \le \alpha;\ 0 \le j \le \alpha \\ \sum_{k=0}^{m} (a_k D^{\alpha}_{j-1,j-1}) x_j^k & \text{for } 0 \le \alpha < i = j \\ \sum_{k=0}^{m} \overset{\alpha}{\oplus} (a_k D^{\alpha}_{i-1,j}) & \text{for } 0 \le \alpha < i;\ 0 \le j < i \\ aD^{\alpha}_{i,j-1} & \text{for } 0 \le \alpha < j;\ 0 \le i < j \end{cases}$$

3.5 The D Modeling Theorem Proofs

The main result of this section is theorem <3.5.11>: $D^{\alpha}_{i,j} : I_i \xrightarrow{H} J^{\alpha}_{j}$. Again, the proofs presented are not required for the developments in later chapters and consequently can be skipped if the reader will accept the validity of the above theorem.

Lemma: $I^{\infty}_{0,0} = F_0$
<3.5.01>

Proof: $I^{\infty}_{0,0} \subseteq F_0$ since $a \in I_0 \Rightarrow aD^{\alpha}_{0,0} = aC_{0,0} \in F_0$ by <3.3.02>. Let $b \in F_0$. Then $bD^{\alpha}_{0,0} = bC_{0,0} = b$ by <3.3.06>. $\therefore F_0 \subseteq I^{\infty}_{0,0}$.

Lemma: $a \in J^{\alpha}_{j} \Rightarrow aD^{\alpha}_{j,j} = a$
<3.5.02>

Proof: Case 1: $0 \leq j \leq \alpha$

$a \in J_j^\alpha \subseteq I_j$ by <2.5.53> and $aD_{j,j}^\alpha = aC_{j,j} = a$ by <3.3.06>.

Case 2: $0 \leq \alpha < j$

Let $h = j - \alpha$ for a fixed α. For $h = 0$, $aD_{j,j}^\alpha = a$ by case 1. Suppose that for some $h \geq 0$ that $b \in J_j^\alpha$ implies $bD_{j,j}^\alpha = b$. Let $a \in J_{j+1}^\alpha$; $a = \sum_{k=0}^{m} a_k x_{j+1}^k$; $a_k \in J_j^\alpha$. Then $a \in I_{j+1}$ and $a_k \in I_j$.

$$aD_{j+1,j+1}^\alpha = \sum_{k=0}^{m} (a_k D_{j,j}^\alpha) x_{j+1}^k = \sum_{k=0}^{m} (a_k) x_{j+1}^k \quad \text{by the inductive hypothesis}$$

$$= a$$

By induction on h, the lemma holds for this case.

Lemma: $J_j^\alpha \subseteq I_{j,j}^\alpha$
<3.5.03>

Proof: Let $a \in J_j^\alpha$. Then $a \in I_j$ and $aD_{j,j}^\alpha = a$ by <3.5.02>. Hence $a \in I_{j,j}^\alpha$ and $J_j^\alpha \subseteq I_{j,j}^\alpha$.

Lemma: $a \in I_j \Rightarrow aD_{i,j}^\alpha = aD_{j,j}^\alpha$; $0 \leq j \leq i$
<3.5.04>

Proof: Case 1: $0 \leq j \leq i \leq \alpha$

$a \in I_j \subseteq I_i \Rightarrow aD_{i,j}^\alpha = aC_{i,j} = aC_{j,j} = aD_{j,j}^\alpha$ by <3.3.19>.

Case 2: $0 \leq j \leq \alpha < i$

Let $h = i - \alpha$ for some fixed α and j. $a \in I_j \Rightarrow a \in I_i$ and $\deg_i(a) = 0$ by <2.4.05>. Assume that for some $h > 0$

$aD^{\alpha}_{i,j} = aD^{\alpha}_{j,j}$. Since $a \in I_{i+1}$, $\deg_{i+1}(a) = 0$ and $aD^{\alpha}_{i+1,j} = \sum_{k=0}^{Q} \overset{\alpha}{\oplus} (aD^{\alpha}_{i,j}) = aD^{\alpha}_{i,j} = aD^{\alpha}_{j,j}$ by the inductive hypothesis. For $h = 1$, $i = \alpha + 1$ and $aD^{\alpha}_{\alpha+1,j} = aD^{\alpha}_{\alpha,j} = aD^{\alpha}_{j,j}$ by case 1. Hence the lemma holds for this case by induction on h.

Case 3: $0 \leq \alpha < j \leq i$

Let $h = i - j$ for some fixed j. For $h = 0$, the lemma holds trivially. Assume that for some $h \geq 0$, $aD^{\alpha}_{i,j} = aD^{\alpha}_{j,j}$. $a \in I_{i+1}$ by <2.4.03> and $\deg_{i+1}(a) = 0$. Therefore $aD^{\alpha}_{i+1,j} = aD^{\alpha}_{i,j} = aD^{\alpha}_{j,j}$ by the inductive hypothesis.

Lemma: $a \in J^{\alpha}_{j} \Rightarrow aD^{\alpha}_{i,j} = a$, $0 \leq j \leq i$
<3.5.05>

Proof: Case 1: $0 \leq j = i$ Directly by <3.5.02>.

Case 2: $0 \leq j < i$

$a \in J^{\alpha}_{j} \Rightarrow a \in I_{j}$ by <2.5.53> and $aD^{\alpha}_{i,j} = aD^{\alpha}_{j,j} = a$ by <3.5.04> and <3.5.02>.

Lemma: $I^{\alpha}_{j,j} = J^{\alpha}_{j}$
<3.5.06>

Proof: $J^{\alpha}_{j} \subseteq I^{\alpha}_{j,j}$ by <3.5.03>.

Case 1: $0 \leq j \leq \alpha$

$D^{\alpha}_{i,j} = C_{j,j} \Rightarrow I^{\alpha}_{j,j} = I^{\infty}_{j,j} = F_{j} = J^{\alpha}_{j}$ <3.3.15>.

Case 2: $0 \leq \alpha < j$

Let $h = j - \alpha$. For $h = 1$, let $a \in I_{\alpha+1}$: $a = \sum_{k=0}^{m} a_k x^{k}_{\alpha+1}$:

$a_k \in I_\alpha \Rightarrow aD^\alpha_{\alpha+1,\alpha+1} = \sum_{k=0}^{m} (a_k D^\alpha_{\alpha,\alpha}) x^k_{\alpha+1} \in J^\alpha_\alpha[x_{\alpha+1}] = J^\alpha_{\alpha+1}$

since $a_k D^\alpha_{\alpha,\alpha} \in J^\alpha_j$ by case 1. Assume that for some $h > 0$, $I^\alpha_{j,j} \subseteq J^\alpha_j$. Let $a \in I_{j+1}$: $a = \sum_{k=0}^{m} a_k x^k_{j+1}$. Then $aD^\alpha_{j+1,j+1} = \sum_{k=0}^{m} (a_k D^\alpha_{j,j}) x^\alpha_{j+1} \in J^\alpha_j[x_{j+1}] = J^\alpha_{j+1}$ since by the inductive hypothesis $a_k D^\alpha_{j,j} \in J^\alpha_j$. By induction on h, the case holds. Hence $I^\alpha_{j,j} \subseteq J^\alpha_j$ for $0 \leq \alpha$, $0 \leq j$ implying $I^\alpha_{j,j} = J^\alpha_j$.

Lemma: $D^\alpha_{i,j} = D^\alpha_{i,i}$, $0 \leq i \leq j$
<3.5.07>

Proof: Let $a \in I_i$

Case 1: $0 \leq i \leq j \leq \alpha$

$aD^\alpha_{i,j} = aC_{i,j} = aC_{i,i} = aD^\alpha_{i,i}$ by <3.3.18>.

Case 2: $0 \leq i \leq \alpha < j$

Let $h = j - \alpha$ for some fixed i and α. For $h = 1$, $aD^\alpha_{i,\alpha+1} = aD^\alpha_{i,\alpha} = aD^\alpha_{i,i}$ by case 1. Assume that for some $h > 0$, $aD^\alpha_{i,j} = aD^\alpha_{i,i}$. Then $aD^\alpha_{i,j+1} = aD^\alpha_{i,j} = aD^\alpha_{i,i}$ and hence the case holds by induction.

Case 3: $0 \leq \alpha < i \leq j$

Let $h = j - i$ for a fixed α and i. For $h = 0$, the lemma holds trivially. Assume that for some $h > 0$, $aD^\alpha_{i,j} = aD^\alpha_{i,i}$. Then $aD^\alpha_{i,j+1} = aD^\alpha_{i,j} = aD^\alpha_{i,i}$.

Lemma: $I^\alpha_{i,j} = J^\alpha_i$, $0 \leq i \leq j$
<3.5.08>

Proof: $D^{\alpha}_{i,j} = D^{\alpha}_{i,i}$ by <3.5.07> => $I^{\alpha}_{i,j} = I^{\alpha}_{i,i} = J^{\alpha}_{i}$ by <3.5.06>.

Lemma: $I^{\alpha}_{i,j} = J^{\alpha}_{j}$, $0 \leq j \leq i$ <3.5.09>

Proof: $J^{\alpha}_{j} \subseteq I^{\alpha}_{i,j}$ by <3.5.05>. We must establish that $I^{\alpha}_{i,j} \subseteq J^{\alpha}_{j}$.

Case 1: $0 \leq j \leq i \leq \alpha$

In this region $D^{\alpha}_{i,j} = C_{i,j}$. Hence $I^{\alpha}_{i,j} = I^{\infty}_{i,j} = F_j = J^{\alpha}_{j}$ by <3.3.15>.

Case 2: $0 \leq j \leq \alpha < i$

Let $h = i - \alpha$ for some fixed α. For $h = 1$, let $a \in I^{\alpha}_{\alpha+1,j}$; $a = \sum_{k=0}^{m} \overset{\alpha}{\oplus} (a_k)$ where $a_k \in I^{\alpha}_{\alpha,j} = F_j$ by case 1. Therefore $a = \sum_{k=0}^{m} \overset{j}{\oplus} (a_k) \in F_j = J^{\alpha}_{j}$ by <2.5.23> and <2.5.54>. Consequently $I^{\alpha}_{\alpha+1,j} \subseteq J^{\alpha}_{j}$. Assume that for some $h > 0$, $I^{\alpha}_{i,j} \subseteq J^{\alpha}_{j}$. Let $a \in I^{\alpha}_{i+1,j}$. Then $a = \sum_{k=0}^{m} \overset{\alpha}{\oplus} (a_k)$ where $a_k \in I^{\alpha}_{i,j} \subseteq J^{\alpha}_{j} = F_j$ by the inductive hypothesis. Therefore $a = \sum_{k=0}^{m} \overset{j}{\oplus} (a_k) \in F_j = J^{\alpha}_{j}$ by <2.5.23>, <2.5.54>. Therefore $I^{\alpha}_{i+1,j} \subseteq J^{\alpha}_{j}$ and the case holds by induction on h.

Case 3: $0 \leq \alpha < j \leq i$

Let $h = i - j$. For $h = 0$, $I^{\alpha}_{j,j} = J^{\alpha}_{j}$ by <3.5.04>. Assume that for some $h \geq 0$, $I^{\alpha}_{i,j} = J^{\alpha}_{j}$. Let $a \in I^{\alpha}_{i+1,j}$. Then $a = \sum_{k=0}^{m} \overset{\alpha}{\oplus} (a_k)$; $a_k \in I^{\alpha}_{i,j} \subseteq J^{\alpha}_{j}$. Therefore

$a = \sum_{k=0}^{m} \overset{\alpha}{\oplus} (a_k) \in J_j^\alpha$ by <2.5.54> and $I_{i+1,j}^\alpha \subseteq J_j^\alpha$. Hence $I_{i,j}^\alpha \subseteq J_j^\alpha$ for all cases.

<u>Theorem</u>: $I_{i,j}^\alpha \subseteq J_j^\alpha$
<3.5.10>

Proof: Case 1: $0 \leq j \leq i$: $I_{i,j}^\alpha = J_j^\alpha$ by <3.5.09>.

Case 2: $0 \leq i < j$: $I_{i,j}^\alpha = J_i^\alpha \subseteq J_j^\alpha$ by <3.5.08> and <2.5.53>.

<u>Theorem</u>: $D_{i,j}^\alpha : I_i \xrightarrow{H} J_j^\alpha$
<3.5.11>

Proof: Case 1: $0 \leq j \leq i \leq \alpha$

Since $D_{i,j}^\alpha = C_{i,j}$ in this region the theorem is true by <3.3.25>.

Case 2: $0 \leq \alpha < i = j$

Let $h = j - \alpha$ for some fixed α. Let $a,b \in I_{j+1}$:

$a = \sum_{k=0}^{K} a_k x_{j+1}^k$; $a_k \in I_j$ and $b = \sum_{m=0}^{M} b_m x_{j+1}^m$; $b_m \in I_j$. Define $N = \max(K,M)$ and assume that $D_{j,j}^\alpha : I_j \xrightarrow{H} J_j^\alpha$.

$$aD_{j+1}^\alpha \overset{\alpha}{\oplus} bD_{j+1}^\alpha$$
$$= \left(\sum_{k=0}^{K} a_k D_{j,j}^\alpha x_{j+1}^k\right) \overset{\alpha}{\oplus} \left(\sum_{m=0}^{M} b_m D_{j,j}^\alpha x_{j+1}^k\right)$$
$$= \left(\sum_{n=0}^{N} \overset{\alpha}{\oplus} (a_n D_{j,j}^\alpha) x_{j+1}^n\right) \overset{\alpha}{\oplus} \left(\sum_{n=0}^{N} \overset{\alpha}{+} (b_n D_{j,j}^\alpha) x_{j+1}^n\right) \text{ by } \langle 2.2.30\rangle\langle 3.5.10\rangle$$

$$= \sum_{n=0}^{N} \overset{\alpha}{\oplus} (a_n D^{\alpha}_{j,j} \overset{\alpha}{\oplus} b_n D^{\alpha}_{j,j}) x^n_{j+1} \quad \text{by } \langle 2.5.54 \rangle$$

$$= \sum_{n=0}^{N} \overset{\alpha}{\oplus} ((a_n + b_n) D^{\alpha}_{j,j}) x^n_{j+1} \quad \text{by the inductive hypothesis}$$

$$= (a + b) D^{\alpha}_{j,j}$$

$$a D^{\alpha}_{j+1,j+1} \overset{\alpha}{\odot} b D^{\alpha}_{j+1,j+1}$$

$$= \sum_{k=0}^{K} \overset{\alpha}{\oplus} (a_k D^{\alpha}_{j,j}) x^k_{j+1} \overset{\alpha}{\odot} \sum_{m=0}^{M} \overset{\alpha}{\oplus} (b_m D^{\alpha}_{j,j}) x^m_{j+1} \quad \text{by } \langle 2.2.30 \rangle$$

$$= \sum_{n=0}^{K+M} \overset{\alpha}{\oplus} \Big(\sum_{k+m=n} \overset{\alpha}{\oplus} (a_k D^{\alpha}_{j,j} \overset{\alpha}{\odot} b_m D^{\alpha}_{j,j}) \Big) x^n_{j+1} \quad \text{by } \langle 3.5.10 \rangle, \langle 2.5.54 \rangle$$

$$= \sum_{n=0}^{K+M} \overset{\alpha}{\oplus} \Big(\sum_{k+m=n} \overset{\alpha}{\oplus} ((a_k \circ b_n) D^{\alpha}_{j,j}) \Big) x^n_{j+1} \quad \text{by the inductive hypothesis}$$

$$= \sum_{n=0}^{K+M} \overset{\alpha}{\oplus} \Big(\Big[\sum_{k+m=n} (a_k \circ b_m) \Big] D^{\alpha}_{j,j} \Big) x^n_{j+1} \quad \text{by the inductive hypothesis}$$

$$= \sum_{n=0}^{K+M} \Big(\Big[\sum_{k+m=n} (a_k \circ b_m) \Big] D^{\alpha}_{j,j} \Big) x^n_{j+1}$$

$$= (a \circ b) D^{\alpha}_{j+1,j+1}$$

Since $D^{\alpha}_{\alpha,\alpha} : I_{\alpha} \xrightarrow{H} J^{\alpha}_{\alpha}$ by case 1, $D^{\alpha}_{\alpha+1,\alpha+1} : I_{\alpha+1} \xrightarrow{H} J^{\alpha}_{\alpha+1}$. By induction on h, the theorem holds for this case.

Case 3: $0 \leq j \leq \alpha < i$

Let $a, b \in I_{i+1}$; $a = \sum_{k=0}^{K} a_k x^k_{i+1}$; $a_k \in I_i$ and $b = \sum_{m=0}^{M} b_m x^m_{i+1}$;

$b_m \in I_i$. Define $N = \max(K,M)$ and assume that
$D^{\alpha}_{i,j} : I_i \xrightarrow{H} J^{\alpha}_j$ for some $i > \alpha$.

$$aD^{\alpha}_{i+1,j} \overset{\alpha}{\odot} bD^{\alpha}_{i+1,j}$$

$$= \sum_{k=0}^{K} \overset{\alpha}{\oplus} (a_k D^{\alpha}_{i,j}) \overset{\alpha}{\odot} \sum_{k=0}^{M} \overset{\alpha}{\oplus} (b_m D^{\alpha}_{i,j})$$

$$= \sum_{n=0}^{K+M} \overset{\alpha}{\oplus} \Big(\sum_{k+m=n} \overset{\alpha}{\oplus} (a_k D^{\alpha}_{i,j} \overset{\alpha}{\odot} b_m D^{\alpha}_{i,j}) \Big) \quad \text{by } \langle 3.5.09 \rangle, \langle 2.5.24 \rangle$$

$$= \sum_{n=0}^{K+M} \overset{\alpha}{\oplus} \Big(\sum_{k+m=n} \overset{\alpha}{\oplus} ((a_k \circ b_m) D^{\alpha}_{i,j}) \Big) \quad \text{by the inductive hypothesis}$$

$$= \sum_{n=0}^{K+M} \overset{\alpha}{\oplus} \Big(\Big[\sum_{k+m=n} (a_k \circ b_m) \Big] D^{\alpha}_{i,j} \Big) \quad \text{again by the inductive hypothesis}$$

$$= (a \circ b) D^{\alpha}_{i+1,j}$$

By a similar argument

$$aD^{\alpha}_{i,j} \overset{\alpha}{\oplus} bD^{\alpha}_{i,j} = (a + b)D^{\alpha}_{i,j}$$

Let $h = i - \alpha$. For $h = 1$, $D^{\alpha}_{i,j} : I_i \xrightarrow{H} J^{\alpha}_j$ since $D^{\alpha}_{\alpha,j} : I_{\alpha} \xrightarrow{H} J^{\alpha}_j$ by case 1. By induction on h, $D^{\alpha}_{i,j} : I_i \xrightarrow{H} J^{\alpha}_j$ for $0 \leq j \leq \alpha < i$.

Case 4: $0 \leq \alpha < j < i$

Let $a,b \in I_{i+1}$ and defined as in case 3. By the same reasoning as in case 3, we get

$$aD^{\alpha}_{i,j} \overset{\alpha}{\oplus} bD^{\alpha}_{i,j} = (a + b)D^{\alpha}_{i,j}$$

$$aD^{\alpha}_{i,j} \overset{\alpha}{\odot} bD^{\alpha}_{i,j} = (a \cdot b)D^{\alpha}_{i,j}$$

This time let $h = i - j$. For $h = 1$, $D^{\alpha}_{j+1,j} : I_{j+1} \xrightarrow{H} J^{\alpha}_{j}$ since $D^{\alpha}_{j,j} : I_{j} \xrightarrow{H} J^{\alpha}_{j}$ by case 2. Case 4 then holds by induction on h.

Case 5: $0 \leq i < j$

$D^{\alpha}_{i,j} = D^{\alpha}_{i,i} : I_{i} \xrightarrow{H} J^{\alpha}_{i} \subseteq J^{\alpha}_{j}$ by <3.5.07> and <2.5.53>

3.6 The Recursive Modeling Function and its Components

Now that we have defined all the domains of interest and have proven the modeling functions to be homomorphisms, it is convenient to draw all the results together by looking at them in a different manner than that required for the formal definitions and the proofs of the theorems. It is shown that $D^{\alpha}_{i,j}$ can be expressed independent of $C_{i,j}$ and that the C functions are a subclass of the D functions. This relationship allows us to call the $D^{\alpha}_{i,j}$ function in its new formulation "the recursive modeling function". Two auxiliary functions defined as component functions of the $D^{\alpha}_{i,j}$ function will be introduced for the purpose of describing a modeling algorithm when the polynomials being manipulated are in the sum of products form rather than in the recursive form.

Lemma: $C'_{i,j} = D^{j-1}_{i,j}$, $0 \leq j \leq i$
<3.6.01>

Proof: Case 1: $0 = i = j$: Let $a \in I_0$, $aD^{-1}_{0,0} = a = aC'_{0,0}$

Case 2: $0 < i = j$: Let $a \in I_j$, $a = \sum_{k=0}^{m} a_k x_j^k$,

$a_k \in I_{j-1}$.

$$aD^{j-1}_{j,j} = \sum_{k=0}^{m} (a_k D^{j-1}_{j-1,j-1}) x_j = \sum_{k=0}^{m} (a_k C_{j-1,j-1}) = aC'_{i,j}$$

Case 3: $0 \leq j < i$: Let $h = i - j$ and assume that for some $h \geq 0$ $D^{j-1}_{i,j} = C'_{j,j}$. Let $a \in I_{i+1}$, $a = \sum_{k=0}^{m} a_k x_{i+1}^k$, $a_k \in I_i$.

$$aD^{j-1}_{i+1,j} = \sum_{k=0}^{m} {}^{j-1}\oplus (a_k D^{j-1}_{i,j}) = \sum_{k=0}^{m} {}^{j-1}\oplus (a_k C'_{i,j}) = aC'_{i+1,j}.$$

Therefore the lemma holds by case 1 and 2 and induction on h.

Lemma: $C'_{i,j} = D^{i}_{i,i}$, $0 < i < j$
<3.6.02>

Proof: $C'_{i,j} = C_{i,i} = D^{i}_{i,i}$ by <3.3.05>.

Lemma: $D^{\alpha}_{i,j} = D^{j}_{i,j}$, $0 \leq j \leq \alpha$
<3.6.03>

Proof: Case 1: $0 \leq j \leq \alpha$, $0 \leq i \leq j$: $D^j_{i,j} = C_{i,j} = D^\alpha_{i,j}$.

Case 2: $0 \leq j \leq \alpha$, $j < i$: Let $h = \alpha - j$ and assume that for some $h \geq 0$, $D^\alpha_{i,j} = D^j_{i,j}$. Let $a \in I_{i+1}$, $a = \sum_{k=0}^{m} a_k x_{i+1}^k$, $a_k \in I_i$.

$$aD^\alpha_{i+1,j} = \sum_{k=0}^{m} \overset{\alpha}{\oplus} (a_k D^\alpha_{i,j}) = \sum_{k=0}^{m} \overset{j}{\oplus} (a_k D^j_{i,j}) = aD^j_{i+1,j} \quad \text{by } \langle 2.5.23 \rangle$$

and the inductive hypothesis. The lemma holds by induction on h.

Lemma: $C_{i,j} = D^{j-1}_{i,j} M_j$ <3.6.05>

Proof: Case 1: $0 \leq j \leq i$: $D^{j-1}_{i,j} M_j = C'_{i,j} M_j = C_{i,j}$.

Case 2: $0 < i < j$: $D^{j-1}_{i,j} = D^{j-1}_{i,i} = D^i_{i,i} = C'_{i,j}$; $D^{j-1}_{i,j} M_j = C_{i,j}$ by <3.5.07>, <3.6.03> and <3.6.02>.

Corollary: $D^j_{i,j} = D^{j-1}_{i,j} M_j$ <3.6.06>

Theorem: The modeling functions can be rewritten in the following form: <3.6.07>

$$D^\alpha_{i,j} : I_i = J_i^{-1} \xrightarrow{H} J^\alpha_j, \; -1 \leq \alpha; \quad C_{i,j} : J_i^{-1} \xrightarrow{H} J^j_j = F_j.$$

Let $a \in J_i^{-1}$; for $0 < i$ let $a = \sum_{k=0}^{m} a_k x_i^k$, $a_k \in J_{i-1}^{-1}$.

$$aD^{\alpha}_{i,j} = \begin{cases} a & (1)\quad -1 \le \alpha < i \le j \\ aD^{j-1}_{j,j}M_j & (2)\quad 0 \le i = j \le \alpha \\ \sum_{k=0}^{m} (a_k D^{\alpha}_{j-1,j-1})x^k_j & (3)\quad 0 \le \alpha < i = j \\ \sum_{k=0}^{m} \overset{\alpha}{\oplus} (a_k D^{\alpha}_{i-1,j}) & (4)\quad 0 \le j < i,\ -1 \le \alpha \\ aD^{\alpha}_{i,i} & (5)\quad 0 < i < j \end{cases}$$

$$C_{i,j} = D^{j}_{i,j} = D^{\infty}_{i,j}$$

Proof: Case 1 in definition <3.4.01> (the region $0 \le i \le \alpha$, $0 \le j \le \alpha$) can be replaced by the following:

$$aD^{\alpha}_{i,j} = \begin{cases} a & -1 = \alpha,\ 0 = i = j \\ aD^{j-1}_{j,j}M_j & 0 \le j = i \le \alpha \\ aD^{j}_{i,j} = \sum_{k=0}^{m} \overset{\alpha}{\oplus} (a_k D^{\alpha}_{i-1,j}) & 0 \le j < i \le \alpha \\ aD^{i}_{i,i} = aD^{\alpha}_{i,i} & 0 < i < j \le \alpha \end{cases}$$

by the use of lemmas <3.6.01> to <3.6.06>. After the replacement the $D^{\alpha}_{i,j}$ functions appear as follows:

$$aD^{\alpha}_{i,j} = \begin{cases} a & -1 = \alpha,\ 0 = i = j \\ aD^{j-1}_{j,j}M_j & 0 \leq j = i \leq \alpha \\ \sum_{k=0}^{m} (a_k D^{\alpha}_{j-1,j-1}) x^k_j & 0 \leq \alpha < i = j \\ \sum_{k=0}^{m} \overset{\alpha}{\oplus} (a_k D^{\alpha}_{i-1,j}) & 0 \leq j < i \\ aD^{\alpha}_{i,i} & 0 < i < j \end{cases}$$

By the addition of the $\alpha = -1$ case as defined in <2.4.06> the desired formulation is obtained.

Definition: <3.6.10> The modularization modeling function $D^{h,\alpha}_{M_i}$ is defined as $D^{h,\alpha}_{M_i} : J^h_i \longrightarrow J^{\alpha}_i$ for $-1 \leq h \leq \alpha \leq i,\ 0 \leq i$. Let $a \in J^h_i$. $a \in J^{-1}_i$ by <2.5.51> so we can define $aD^{h,\alpha}_{M_i} = aD^{\alpha}_{i,i}$.

Definition: <3.6.11> The substitution modeling function $D^{\alpha}_{Si,j}$ is defined as $D^{\alpha}_{Si,j} : J^{\alpha}_i \longrightarrow J^{\alpha}_j$ for $-1 \leq \alpha,\ 0 \leq j < i,\ \alpha \leq j$. Let $a \in J^h_i$. $a \in J^{-1}_i$ so we can again define $aD^{\alpha}_{Si,j} = aD^{\alpha}_{i,j}$.

Since $D^{\alpha}_{i,j} : J^{-1}_i \xrightarrow{H} J^{\alpha}_i$ we can immediately state the following lemmas:

Lemma: <3.6.12> $D^{h,\alpha}_{M_i} : J^h_i \xrightarrow{H} J^{\alpha}_i,\ -1 \leq h \leq \alpha \leq i,\ 0 \leq i$.

Lemma: $D^{\alpha}_{S_{i,j}} : J^{\alpha}_{i} \xrightarrow{H} J^{\alpha}_{j}, \quad -1 \leq \alpha, \ 0 \leq j < i, \ \alpha \leq j.$
<3.6.13>

Lemma: $D^{h,\alpha}_{M_i} D^{\alpha}_{S_{i,j}} = D^{h}_{S_{i,j}} D^{h,\alpha}_{M_j}, \quad -1 \leq h < \alpha \leq j < i.$
<3.6.14>

The purpose and use of the above two functions can be seen more clearly if we consider the cases in which $\alpha = h+1$, $j = i-1$. For $a \in J^{h}_{i}$, $a = \sum_{k=0}^{m} a_k x_i^k$ the modularization and substitution functions reduce to:

$$aD^{h,h+1}_{M_i} = \begin{cases} aM_{h+1} & 0 \leq h+1 = i \\ \sum_{k=0}^{m} (a_k D^{h+1}_{i-1,i-1}) x_i^k & 0 \leq h+1 < i \end{cases}$$

$$aD^{h}_{S_{i,i-1}} = \sum_{k=0}^{m} \overset{h}{\oplus} (a_k) \qquad -1 \leq h < i, \ 0 < i.$$

The modularization function states that x_{h+1} will be modularized and that the degree structure of x_i for $i > h+1$ will remain unchanged. The substitution function states that the coefficients which are in J^{h}_{i-1} are simply summed.

When the polynomials are represented in a computer by a sum of products form successive application of the above modeling functions may be used to obtain the $D^{\alpha}_{i,j}$ model. By lemma <3.6.14> the modularization and substitution functions are commutative which implies that an optimum path may exist which maps a modeled polynomial in J^{-1}_{i} into its model in J^{α}_{i}. This path optimization depends in general on the prime context sequence and on the structure of the polynomial being modeled.

3.7 Summary of Domain and Modeling Relations

To summarize the relations among the I_i, J_j^α and F_j sets of integral domains, the following schematic can be studied:

$\alpha \longrightarrow$	-1	0	1	2	3	4	$\longrightarrow$	
i								
0	J_0^{-1}	J_0^0					$I_i = J_i^{-1}$	$0 \leq i$
1	J_1^{-1}	J_1^0	J_1^1				$J_1^\alpha = F_j$	$0 \leq j \leq \alpha$
2	J_2^{-1}	J_2^0	J_2^1	J_2^2			$J_j^\alpha = J_{j-1}^\alpha[x_j]$	$-1 \leq \alpha < j$
3	J_3^{-1}	J_3^0	J_3^1	J_3^2	J_3^3			
4	J_4^{-1}	J_4^0	J_4^1	J_4^2	J_4^3	J_4^4		
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\cdots$	
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\cdots$	
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\cdots$	

The set at coordinate (i,α) can be thought of as having an adjunction level of i and a modularity of α, where the adjunction level is the number of indeterminates in the domain and the modularity specifies the indeterminate which is the last one in a finite field. In other words, the integral domain at (i,α) has i indeterminates and if $\alpha > 0$, the degrees of indeterminates $x_1, x_2, \ldots, x_\alpha$ has been reduced by modularization whereas the degrees of the indeterminates $x_{\alpha+1}, \ldots, x_j$ are still possibly intact after modeling.

The above schematic provides a good visualization of neighboring set relations. Define the following symbols:

C - Center set: Set about which we are talking - (eg. (3,1))

L - Neighbor set to the left of C - (3,0)

A - Set above C - (2,1)

R - Set to the right of C - (3,2)

B - Set below C - (4,1)

The set relations then are given by the following:

L includes C

A C is defined by the adjunction of x_i to A.
C includes A by an embedding.

R is included in C

B is an adjunction of C. B includes C by an embedding.

Let a be an element of C. Then a can be mapped into any of the 4 neighboring sets by functions which we can give the following names:

C	to L	Reconstruction	$(a \in C \Rightarrow a \in L)$
C	to A	Substitution	$(D^{\alpha}_{S_{i,i-1}})$
C	to R	Modularization	$(D^{\alpha,\alpha+1}_{M_i})$
C	to B	Embedding	

The mappings from C to A and C to R are the modeling functions and the others are the identity function for the cases we have so far considered. All 4 mappings are homomorphisms.

The reconstruction mapping which we need is only the identity function and hence information lost during the modeling is not recovered. In a more complicated situation this information can be reconstructed. For example, the J_0^{-1} to J_0^0 modularization is commonly called residue coding which has been proposed as a number system for arithmetic operations in a computer[7]. In this case a number of models (each with a different p_0) are formed; the arithmetic processes are performed in the model domain and subsequently the result is "reconstructed" by the use of the Chinese remainder theorem.

The C to A function is termed a 'substitution' rather than a summation since elements in J_{i-1}^{α} other than the unit can be substituted for x_i to produce the C to A function. If we substitute $\beta \in J_{i-1}^{\alpha}$ for x_i we are essentially finding the remainder modulo the prime polynomial $(x_i-\beta)$ which is equivalent to the modularization from C to R. But, since the practicality of generalizing this to a modularization with a higher degree prime polynomial seems questionable, we refrain from calling the C to A substitution also a modularization.

CHAPTER IV AUGMENTED MODELING

4.1 Introduction

The D modeling functions developed in Chapter 3 have the ability of producing models in which the degree information of selected indeterminates is kept intact. However, it will sometimes happen that some of the non-zero coefficients of a modeled polynomial will be in the ideal $(p_0, p_1, p_2, \ldots, p_\alpha)$, the kernel of the $D^{\alpha}_{i,j}$ modeling function. When this polynomial is mapped into J^{α}_{i}, $0 \leq \alpha < i$ the corresponding coefficients in the model polynomial will be zero. If the leading coefficient is in the kernel, the degree of the model polynomial is lower than that of the modeled polynomial a circumstance which can cause an algorithm to produce erroneous results when the internal branching is controlled by the degree information as, for example, in the division and g.c.d. algorithms.

There are a number of possible solutions to this predicament. The first and most obvious is to use a very large prime for p_0 and high degree prime polynomials for the rest of the elements in the prime context sequence. This reduces the probability of producing a non-zero element of the $D^{\alpha}_{i,j}$ kernel during a computation to an insignificantly small value. It may then be assumed that the degree of the model will always be the same as the degree of the modeled polynomial and that the production of a zero in the model implies that the corresponding modeled polynomial is also zero. In some

instances this approach may be satisfactory, but it is too inefficient, often dangerous and somewhat inelegant for general use.

A second solution is to add a "virtual degree" augmentation to the model in order to be able to detect when the leading coefficient of the modeled polynomial is in the kernel of the modeling, the condition under which the model will be called "degree reduced". This is the approach which is developed in what follows. It will be shown that the degree information can be treated algebraically in a manner closely related to discrete exponential valuations[11]. The virtue of this approach is that an algorithm in the augmented model domains is capable of detecting when too much degree information is lost to continue. Often the algorithm can proceed to its natural termination point in which case some information about the result of applying the equivalent algorithm to the modeled polynomial is obtained. In particular, the "model conclusive g.c.d. theorem" developed in this chapter shows that the g.c.d. algorithm can be applied in the model domains and that the algorithm is capable of determining conclusively that two polynomials are relatively prime if no degree reduced polynomial remainder is encountered.

4.2 The Augmented Modeling Domains and Functions

In this section we define a set of augmented modeling domains which consist of the J domains to which a 'virtual

degree' augmentation has been added. Once these domains are available, sets of functions are defined on them which prescribe exactly the operations to be performed on the J domain component and the virtual degree component of an element in the augmented domain when the function is applied. Next we introduce the concept of a 'valuation preserving homomorphic' (or VPH) function which is roughly equivalent to stating that a function having this property commutes with the augmented D_M modularization modeling function. The usefulness of this concept stems from the fact that composite VPH functions can be generated by argument dependent algorithms composed of VPH functions and defined only on the augmented model domains. In other words, an algorithm can proceed in the model domain as long as only VPH functions are met and at each point the accumulated composite function has generated polynomials in the model domain which are identical to the model polynomials which would be obtained by applying the D_M modeling function to the polynomials in the modeled domains which are generated by the equivalent accumulated composite function on the modeled domains.

These concepts are not developed to the full generality possible; efforts are concentrated on obtaining a set of definitions and relations which are sufficient to rigorously prove the model conclusive g.c.d. theorem.

<u>Definition</u>: <4.2.01> (Extension of the degree function $\deg_j(a)$, $a \in I_i$ as defined in <2.4.05>) $\delta^{\alpha}_{i,j} : J^{\alpha}_i \longrightarrow U$. $a \in J^{\alpha}_i \Rightarrow a \in I_i$. Define

$$a\delta^{\alpha}_{i,j} = \begin{cases} \deg_\infty (a) & 0 \leq i = j \leq \alpha \\ \deg_j (a) & (-1 \leq \alpha < i = j) \text{ or } (-1 \leq \alpha, 0 \leq j < i) \\ \deg_\infty (a) & 0 \leq \alpha; 0 \leq i < j \end{cases}$$

Note that $\deg_j (a)$ was defined on elements in I_i so here we first map the elements from J^{α}_i into I_i and then apply the degree function. Also, for $\alpha = -1$, $a\delta^{-1}_{i,j} = \deg_j (a)$.

<u>Definition</u>: <4.2.02> Define the two functions $\overset{u}{\oplus}$ and $\overset{u}{\odot}$ by the following:

$$\overset{u}{\oplus} : U \times U \longrightarrow U, \quad (a,b)\overset{u}{\oplus} = \max(a,b) = a \overset{u}{\oplus} b$$
$$\overset{u}{\odot} : U \times U \longrightarrow U, \quad (a,b)\overset{u}{\odot} = a \overset{u}{\odot} b = a + b$$

where U was defined in <2.6.07>.

<u>Lemma</u>: <4.2.03> $\{U, \overset{u}{\oplus}\}$ and $\{U, \overset{u}{\odot}\}$ are commutative monoids with $-\infty$ as the additive $(\overset{u}{\oplus})$ identity and 0 as the multiplicative $(\overset{u}{\odot})$ identity.
$a,b,c \in J^{\alpha}_i \Rightarrow a \overset{u}{\odot} (b \overset{u}{\oplus} c) = (a \overset{u}{\odot} b) \overset{u}{\oplus} (a \overset{u}{\odot} c)$.

Proof: Closure and associativity follow from the definitions and since $\max((a,b),c) = \max(a,b,c)$. $-\infty$ is the additive identity since $\forall a \in J_i^{\alpha}$, $a \overset{u}{\oplus} (-\infty) = \max(a,-\infty) = a$. Similarly $a \overset{u}{\odot} 0 = a + 0 = a$. Distribution follows from:

$$\begin{aligned}(a \overset{u}{\odot} b) \overset{u}{\oplus} (a \overset{u}{\odot} c) &= \max(a + b,\ a + c) \\ &= a + \max(b,c) \\ &= a \overset{u}{\odot} (b \overset{u}{\oplus} c).\end{aligned}$$

<u>Definition</u>: <4.2.04> A function $\lambda : R \longrightarrow U$ will be called a valuation homomorphism from the ring $\{R,\oplus,\odot\}$ into U if $\forall a,b \in R$, $(a \oplus b)\lambda \leq a\lambda \overset{u}{\oplus} b\lambda$

$$(a \odot b)\lambda \leq a\lambda \overset{u}{\odot} b\lambda$$

Under these conditions we denote the function λ by $\lambda : R \xrightarrow{V} U$.

<u>Definition</u>: <4.2.045> The 'Virtual Degree' or V-modeling function is defined by the following:

Let $a \in J_i^{-1}$; $a = \sum_{k=0}^{m} a_k x_i^k$ for $0 < i$.

$$aV^{\alpha}_{i,j} = \begin{cases} a\delta^{-1}_{i,j} & (1) \quad -1 = \alpha < i = j \\ a\delta^{-1}_{i,\infty} & (2) \quad 0 \le i = j \le \alpha \\ a\delta^{-1}_{i,i} & (3) \quad 0 \le \alpha < i = j \\ a\delta^{-1}_{i,\infty} & (4)A \quad 0 \le j \le \alpha,\ j < i \\ \overset{m}{\underset{k=0}{\overset{u}{\bigoplus}}} (a_k \delta^{-1}_{i-1,j}) & (4)B \quad -1 \le \alpha < j < i \\ a\delta^{-1}_{i,\infty} & (5) \quad 0 \le \alpha,\ 0 \le i < j \end{cases}$$

Define $V = \{V^{\alpha}_{i,j} \mid V^{\alpha}_{i,j} : J^{-1}_i \longrightarrow U;\ -1 \le \alpha,\ 0 \le i,\ 0 \le j\}$

Lemma: $V^{\alpha}_{i,j} : J^{-1}_i \xrightarrow{V} U$
<4.2.05>

Proof: For all cases but (4)B $(-1 \le \alpha < j < i)$: $aV^{\alpha}_{i,j} = a\delta^{-1}_{i,k}$, $k = i, j$ or ∞.

$$(a + b)V^{\alpha}_{i,j} = (a + b)\delta^{-1}_{i,k} \le \max(a\delta^{-1}_{i,k}, b\delta^{-1}_{i,k}) = aV^{\alpha}_{i,j} \overset{u}{\oplus} bV^{\alpha}_{i,j}$$

$$(a \circ b)V^{\alpha}_{i,j} = (a \circ b)\delta^{-1}_{i,k} = a\delta^{-1}_{i,k} + b\delta^{-1}_{i,k} = aV^{\alpha}_{i,j} \overset{u}{\odot} bV^{\alpha}_{i,j}$$

Case (4)B: $-1 \le \alpha < j < i$: Let $a = \sum_{k=0}^{K} a_k x_i^k$, $b = \sum_{m=0}^{M} b_m x_i^m$, $N = \max(K, M)$.

$$aV^{\alpha}_{i,j} \overset{u}{\oplus} bV^{\alpha}_{i,j} = \sum_{k=0}^{K} \overset{u}{\oplus} (a_k \delta^{-1}_{i-1,j}) \overset{u}{\oplus} \sum_{m=0}^{M} \overset{u}{\oplus} (b_m \delta^{-1}_{i-1,j})$$

$$= \sum_{n=0}^{N} \overset{u}{\oplus} (a_n \delta^{-1}_{i-1,j} \overset{u}{\oplus} b_n \delta^{-1}_{i-1,j}) \qquad \text{by } \langle 4.2.03 \rangle$$

$$= \sum_{n=0}^{N} \overset{u}{\oplus} (\max(a_n \delta_{i-1,j}^{-1}, b_n \delta_{i-1,j}^{-1}))$$

$$\geq \sum_{n=0}^{N} \overset{u}{\oplus} ((a_n + b_n)\delta_{i-1,j}^{-1})$$

$$= (a + b)V_{i,j}^{\alpha}$$

$$aV_{i,j}^{\alpha} \overset{u}{\odot} bV_{i,j}^{\alpha} = \sum_{k=0}^{K} \overset{u}{\oplus} (a_k \delta_{i-1,j}^{-1}) \overset{u}{\odot} \sum_{m=0}^{M} \overset{u}{\oplus} (b_m \delta_{i,j}^{-1})$$

$$= \sum_{n=0}^{K+M} \overset{u}{\oplus} \Big(\sum_{k+m=n} \overset{u}{\oplus} (a_k \delta_{i-1,j}^{-1} \overset{u}{\odot} b_m \delta_{i-1,j}^{-1}) \Big)$$

$$= \sum_{n=0}^{K+M} \overset{u}{\oplus} \Big(\sum_{k+m=n} \overset{u}{\oplus} ([a_k \circ b_m]\delta_{i-1,j}^{-1}) \Big)$$

$$\geq \sum_{n=0}^{K+M} \overset{u}{\oplus} \Big(\Big[\sum_{k+m=n} (a_n \circ b_m) \Big] \delta_{i-1,j}^{-1} \Big)$$

$$= (a \circ b)V_{i,j}^{\alpha}$$

<4.2.06>

Definition: Let $b \in J_i^{-1}$. Define $\mathring{b} = bV_{i,j}^{\alpha} \in U$. Let $a \in J_i^{\alpha}$ and define $\underline{a} = (a, \mathring{a})$ to be the augmentation (or augmented model) of a; a is called the D component (or D-model) of $\underline{a}$ and $\mathring{a}$ the V component (or V-model) of $\underline{a}$. Note that $a = \underline{a}K_0$, $\mathring{a} = \underline{a}K_1$ by <2.6.02>. Define $\underline{J}_i^{\alpha} = \{\underline{a} \mid \underline{a} = (a, \mathring{a}),\ a \in J_i^{\alpha},\ \mathring{a} \in U\}$. Then $\underline{J}_i^{\alpha} \subseteq J_i^{\alpha} \times U$.

It should be observed that the V component is not strictly dependent on the D component. An augmented modeling function will be defined which assigns a value to the V component of every $\underline{a} \in \underline{J}_i^{\alpha}$. Then sets of functions on $\underline{J}_i^{\alpha}$ will

be defined which will prescribe the exact operations to be performed on the D and V components when the function is applied. Hence the two components are related in the sense that the values will always be derived from the same set of modeled polynomials and by the application of a parallel set of functions. The functions defined on $\underline{J}_i^\alpha$ will be such that a and $\mathring{a}$ will always be related by the inequality $a\delta_{i,i}^\alpha \leq \mathring{a}$. Because of this property $\mathring{a}$ can be referred to as the "virtual degree" of a.

Definition: $\underline{0} = (0,-\infty)$, $\underline{1} = (1,0)$, $\underline{-1} = (-1,0)$
<4.2.07>

Definition: The Augmented modeling function is defined by
<4.2.08> $\underline{D}_{i,j}^\alpha : \underline{J}_i^{-1} \longrightarrow \underline{J}_j^\alpha$. Let $a \in J_i^{-1}$, $\mathring{a} \in U$ and $\underline{a} = (a,\mathring{a})$. Then $\underline{a}\underline{D}_{i,j}^\alpha = (aD_{i,j}^\alpha, aV_{i,j}^\alpha)$. Note that the V component of $\underline{a}$ is not used during the modeling. Whenever a modeling is performed a new V component is generated based only on the D component of $\underline{a}$.

Definition: Augmented modularization: $\underline{D}_{M_i}^{h,\alpha} : \underline{J}_i^h \longrightarrow \underline{J}_i^\alpha$,
<4.2.09> $-1 \leq h < \alpha \leq i$. For $\underline{a} \in \underline{J}_i^h$, $\underline{a}\underline{D}_{M_i}^{h,\alpha} = (aD_{M_i}^{h,\alpha}, \mathring{a})$.

Definition: The augmented addition and multiplication func-
<4.2.10> tion $\underline{\oplus}_i^\alpha$ and $\underline{\odot}_i^\alpha$ represented by $\underline{O}_i^\alpha$ are defined

as follows: $\underline{O}_i^\alpha : (\underline{J}_i^\alpha)^2 \longrightarrow \underline{J}_i^\alpha$, $\underline{a},\underline{b} \in \underline{J}_i^\alpha \Rightarrow (\underline{a},\underline{b})\underline{O}_i^\alpha = \underline{a}\,\underline{O}_i^\alpha\,\underline{b} = (a \overset{\alpha}{O} b,\ \dot{a} \overset{u}{O} \dot{b})$

<4.2.11> **Definition**: The degree function on $\underline{J}_i^\alpha$ is defined by $\underline{\delta}_{i,j}^\alpha : \underline{J}_i^\alpha \longrightarrow U$, $\underline{a}\underline{\delta}_{i,j}^\alpha = a\delta_{i,j}^\alpha$.

<4.2.12> **Definition**: The k'th coefficient function: $\underline{\chi}_{i,k}^\alpha : \underline{J}_i^\alpha \longrightarrow \underline{J}_i^\alpha$. For $\underline{a} = (a,\mathring{a}) \in \underline{J}_i^\alpha$, let $a = \sum_{k=0}^{m} a_k x_i^\alpha$ for $i > 0$. Then the augmentation of a_k is $\underline{a}_k = (a_k,\mathring{a}_k)$.

$$\underline{a}\underline{\chi}_{i,k}^\alpha = \begin{cases} (0,-\infty) & (-1 = \alpha,\ 0 = i) \text{ or } (0 \le i \le \alpha) \\ (a_k x_i^0,\mathring{c}) & (-1 = \alpha,\ 0 < i) \text{ or } (0 \le \alpha < i) \end{cases}$$

where $\mathring{c} = 0$ if $\mathring{a}_k \ge 0$; $\mathring{c} = -\infty$ if $\mathring{a}_k = -\infty$.

<4.2.13> **Definition**: Leading coefficient function: $\underline{\ell}_i^\alpha : \underline{J}_i^\alpha \longrightarrow \underline{J}_i^\alpha$. Let $\underline{a} \in \underline{J}_i^\alpha$, $k = \underline{a}K_1 = \mathring{a}$.

$$\underline{a}\underline{\ell}_i^\alpha = \begin{cases} (0,-\infty) & \text{if } k = -\infty \\ \underline{a}\underline{\chi}_{i,k}^\alpha & \text{if } k \ge 0 \end{cases}$$

<4.2.14> **Definition**: Reduction function: $\underline{\rho}_i^\alpha : (\underline{J}_i^\alpha)^2 \longrightarrow \underline{J}_i^\alpha$. Let $\underline{a},\underline{b} \in \underline{J}_i^\alpha$

$$\underset{a}{\overset{b}{\rho}}{}_i^{\alpha} = (a,b)\rho_i^{\alpha} = \begin{cases} (c, \mathring{a}-1) & \text{if } 0 < \mathring{b} \leq \mathring{a},\ \mathring{b} = b\delta_{i,i}^{\alpha}. \\ a & \text{All other cases: } (\mathring{b} \leq 0),\ (\mathring{a} < \mathring{b}),\ b\delta_{i,i}^{\alpha} < \mathring{b}. \end{cases}$$

where $c = [((b \not\in_i^{\alpha}) \odot_i^{\alpha} a) \oplus_i^{\alpha} ((-1) \odot_i^{\alpha} (a \not\in_i^{\alpha}) \odot_i^{\alpha} b \odot_i^{\alpha} x_i^h)]K_0$
and $h = \mathring{a} - \mathring{b}$.

<4.2.15>

Definition: Residue modulo b: $R_i^{\alpha} : (J_i^{\alpha})^2 \longrightarrow J_i^{\alpha}$. Let $a,b \in J_i^{\alpha}$.

$$(a,b)R_i^{\alpha} = a(\overset{b}{\rho}{}_i^{\alpha})^h, \qquad h = \mathring{a} - \mathring{b} + 1$$

Note that the function is well defined even for $h \leq 0$ by <2.6.04>. b is called the divisor of the residue function.

<4.2.16>

Definition: $f_i = \{f_i^{\alpha} \mid f_i^{\alpha} : (J_i^{\alpha})^n \longrightarrow (J_i^{\alpha})^m,\ -1 \leq \alpha \leq i\}$. f_i is called a valuation preserving homomorphic (VPH) set of functions on J_i^{α} and J_i^h if for $a \in (J_i^{\alpha})^n$ and $-1 \leq h < \alpha \leq i$:

$$a \; \underset{\theta}{D_{M_i}^{h,\alpha}} \; f_i^{\alpha} = af_i^h \; \underset{\theta}{D_{M_i}^{h,\alpha}}$$

Define $VPH_i^{h,\alpha} = \{f_i \mid f_i$ is a VPH set of functions on J_i^h, J_i^{α} for $-1 \leq h < \alpha \leq i\}$

Lemma: $f,g \in VPH_i^{h,\alpha} \Rightarrow fg \in VPH_i^{h,\alpha}$
<4.2.17>

Proof: Since $D_{M_i}^{h,\alpha} : J_i^h \xrightarrow{H} J_i^\alpha$ by <3.6.12> the D component equivalence follows immediately. The V component equality follows since $\underline{a}D_{M_i}^{h,\alpha}K_1 = \mathring{a}$.

Lemma: $\underline{\oplus}_i, \underline{\odot}_i \in VPH_i^{h,\alpha}$
<4.2.18>

Proof: Let $\underline{a},\underline{b} \in \underline{J}_i^{h,\alpha}$ and O stand for $\oplus$ or $\odot$.

$$(\underline{a}D_{M_i}^{h,\alpha},\underline{b}D_{M_i}^{h,\alpha})\underline{O}_i^\alpha = ((aD_{M_i}^{h,\alpha} \overset{\alpha}{O} bD_{M_i}^{h,\alpha}), (\mathring{a} \overset{u}{O} \mathring{b}))$$
$$= ((a \overset{h}{O} b)D_{M_i}^{h,\alpha}, (\mathring{a} \overset{u}{O} \mathring{b})) \quad \text{by <3.6.12>}$$
$$= (\underline{a} \underline{O}_i^h \underline{b})\underline{D}_{M_i}^{h,\alpha}$$

Lemma: $\underline{\chi}_{i,k} \in VPH_i^{h,\alpha}$, $-1 \le h < \alpha < i$
<4.2.19>

Proof: Let $\underline{a} \in \underline{J}_i^h$; $\underline{a} = (a,\mathring{a})$, $a = \sum_{k=0}^{m} \overset{h}{\oplus} (a_k x_i^k)$. Then

$$\underline{a}_k = (a_k,\mathring{a}_k),\ aD_{M_i}^{h,\alpha} = \sum_{k=0}^{m} \overset{\alpha}{\oplus} (a_k D_{M_{i-1}}^{h,\alpha})x_i^k$$

$$\underline{a}\underline{\chi}_{i,k}^h \underline{D}_{M_i}^{h,\alpha} = (a_k x_i^0, c)\underline{D}_{M_i}^{h,\alpha} = ((a_k D_{M_{i-1}}^{h,\alpha})x_i^0, c)$$

$$\underline{a}D_{M_i}^{h,\alpha}\underline{\chi}_{i,k}^\alpha = (aD_{M_i}^{h,\alpha},\mathring{a})\underline{\chi}_{i,k}^\alpha = ((a_k D_{M_{i-1}}^{h,\alpha})x_i^0, c)$$

where $c = 0$ if $\mathring{a}_k \ge 0$ and $c = -\infty$ if $\mathring{a}_k = -\infty$

Lemma: $\underline{\mathscr{L}}_i \in VPH_i^{h,\alpha}$
<4.2.20>

Proof: Let $\underline{a} \in \underline{J}_i^h$, $k = \mathring{a} = \underline{a}K_1$. $\underline{a}\underline{D}_{M_i}^{h,\alpha}K_1 = \mathring{a} = k$.
$k = -\infty \Rightarrow a D_{M_i}^{h,\alpha} = a = 0$. For $k = -\infty$,

$$\underline{a}\,\underline{\mathscr{L}}_i^h \underline{D}_{M_i}^{h,\alpha} = \underline{0}\underline{D}_{M_i}^{h,\alpha} = \underline{0}$$

$$\underline{a}\underline{D}_{M_i}^{h,\alpha}\underline{\mathscr{L}}_i^h = (a D_{M_i}^{h,\alpha}, -\infty) = \underline{0}$$

For $k \geq 0$, $\underline{a}\,\underline{\mathscr{L}}_i^h \underline{D}_{M_i}^{h,\alpha} = \underline{a}\underline{\chi}_{i,k}^h \underline{D}_{M_i}^{h,\alpha} = \underline{a}\underline{D}_{M_i}^{h,\alpha}\underline{\chi}_{i,k}^{\alpha} = \underline{a}\underline{D}_{M_i}^{h,\alpha}\underline{\mathscr{L}}_i^{\alpha}$.

Lemma: $(\underline{\rho}_i^{\underline{b}h})\underline{D}_{M_i}^{h,\alpha} = \underline{D}_{M_i}^{h,\alpha}(\underline{\rho}_i^{h})^{\underline{b}\underline{D}_{M_i}^{h,\alpha}}$ if $0 < \underline{b}\delta_{i,i}^h = \mathring{b} = \underline{b}\underline{D}_{M_i}^{h,\alpha}\delta_{i,i}^{\alpha}$
<4.2.21>

Proof: The condition $0 < \underline{b}\delta_{i,i}^{\alpha} = \mathring{b} = \underline{b}\underline{D}_{M_i}^{h,\alpha}\delta$ guarantees that $\underline{b}\,\underline{\mathscr{L}}_i^h \neq 0$ and $\underline{b}\underline{D}_{M_i}^{h,\alpha}\underline{\mathscr{L}}_i^{\alpha} \neq 0$. Let $\underline{a} \in \underline{J}_i^h$.

Case 1: $\mathring{a} < \mathring{b} \Rightarrow \underline{a}(\underline{\rho}_i^{\underline{b}h}) = \underline{a}$, $\underline{a}\underline{D}_{M_i}^{h,\alpha}(\underline{\rho}_i^{h})^{\underline{b}\underline{D}_{M_i}^{h,\alpha}} = \underline{a}\underline{D}_{M_i}^{h,\alpha}$

Case 2: $\mathring{a} \geq \mathring{b}$. The 'c' function in the $\underline{\rho}_i^{\alpha}$ definition <4.2.14> is composed of functions in $VPH_i^{h,\alpha}$ and hence is also in $VPH_i^{h,\alpha}$. The fact that the leading coefficients in b and $bD_{M_i}^{h,\alpha}$ are not zero guarantees that the coefficient of $x_i^{\mathring{a}}$ in c will be zero and hence that the virtual degree can be reduced in both domains.

Theorem: $(\underline{R}_i^{\underline{b}h})\underline{D}_{M_i}^{h,\alpha} = \underline{D}_{M_i}^{h,\alpha}(\underline{R}_i^{\alpha})^{\underline{b}\underline{D}_{M_i}^{h,\alpha}}$ for $\underline{b} \in \underline{J}_i^h$,
<4.2.22>

$0 < \underline{b}\delta^{h}_{i,i} = \overset{\circ}{b} = \underline{bD}^{h,\alpha}_{M_i}\underline{\delta}^{\alpha}_{i,i}$.

Proof: Under the given conditions $(\underline{\rho}^{h}_{i})\underline{D}^{h,\alpha}_{M_i} = \underline{D}^{h,\alpha}_{M_i}(\underline{\rho}^{\alpha}_{i})$. Since $\underline{R}_i$ is a composite consisting of only $\underline{\rho}_i$ functions, the theorem holds.

4.3 The Model Conclusive g.c.d. Theorem

We have available now a sufficient number of functions defined on the augmented domain to generate polynomial remainder sequences in the model domains and to develop the model conclusive g.c.d. theorem with which we are able to show that two polynomials are relatively prime with respect to a specified indeterminate by performing operations only in the model domains. A number of examples are given to demonstrate the power of this theorem and to illustrate some problems which might be encountered when applying the theorem in practical cases.

Definition: <4.3.01> Let $\underline{a},\underline{b},\underline{r} \in \underline{J}^{\alpha}_{i}$, $-1 \leq \alpha < i$, $0 < i$. Then $(\underline{a},\underline{b},\underline{r})$ is called a polynomial remainder triplet (p.r.t.) over $\underline{J}^{\alpha}_{i}$ if $\underline{a}\delta \geq \underline{b}\delta > \underline{r}\delta$ and there exist $\underline{b}',\underline{q},\underline{a}' \in \underline{J}^{\alpha}_{i}$, $\underline{b}' = (b',0)$, $\underline{a}' = (a',0)$ and $b'\delta = a'\delta = 0$ such that $\underline{b}' \odot \underline{a} = (\underline{b} \odot \underline{q}) \oplus (\underline{a}' \odot \underline{r})$. It follows that $\overset{\circ}{a} = \overset{\circ}{b} \overset{u}{\odot} q$. Note that δ is used to represent $\delta^{\alpha}_{i,i}$.

Definition: <4.3.02> $\underline{r} = (\underline{r}_0,\underline{r}_1,\ldots,\underline{r}_n)$ is called a polynomial remainder sequence (p.r.s.) if each triplet

$(\underline{r}_m, \underline{r}_{m+1}, \underline{r}_{m+2})$ is a p.r.t. over J_i^α for $0 \leq m \leq n-2$. $\underline{r}$ is called a normal p.r.s. if $\underline{r}_{m+1}\delta = \underline{r}_m\delta - 1$ for $1 \leq m < n$. $\underline{r}$ is called a complete p.r.s. if $\underline{r}_n K_0 = 0$

The above definitions are consistent with those in references (5) and (6). It is to be noted that the V components were not used in the definitions and hence a p.r.t. and p.r.s. could have been defined only on J_i^α.

<4.3.03> **Theorem:** (Euclidean Algorithm) If $\underline{r}$ is a complete p.r.s. then r_{n-1} is an associate of the g.c.d. of r_0, r_1.

Proof: Since J_i^α is an integral domain, $r_n = 0$ implies r_{n-1} divides associates of r_m for $0 \leq m \leq n-1$. Hence the g.c.d. of r_0, r_1 must be an associate of r_{n-1}.

<4.3.04> **Lemma:** Let $\underline{r} = (\underline{r}_0, \underline{r}_1, \ldots, \underline{r}_n)$ and $\underline{r}_{m+2} = (\underline{r}_m, \underline{r}_{m+1})\underline{R}_i^\alpha$. Then $\underline{r}$ is a p.r.s. if and only if $\mathring{r}_0 \geq r_1$ and $\mathring{r}_m = r_m\delta$ for $1 \leq m < n$. We call $\underline{r}$ the p.r.s. generated by $(\underline{r}_0, \underline{r}_1, \underline{R}_i^\alpha)$.

Proof: Under the condition $r_0 \geq r_1$ and $\mathring{r}_m = r_m\delta$, $\underline{r}_2 = (\underline{r}_0, \underline{r}_1)\underline{R}_i^\alpha$, $\mathring{r}_2 = r_1 - 1$ by definition of the $\underline{R}_i^\alpha$ function and $(\underline{r}_0, \underline{r}_1, \underline{r}_2)$ is a p.r.t. The condition $\mathring{r}_m = r_m\delta$ guarantees that $\underline{r}_3 = (\underline{r}_1, \underline{r}_2)\underline{R}_i^\alpha$. By induction on m, we see that $(\underline{r}_0, \underline{r}_1, \underline{R}_i^\alpha)$ generates $\underline{r}$.

If $\underline{r}$ is generated by $(\underline{r}_0, \underline{r}_1, \underline{R}_i^{\alpha})$, $\mathring{r}_0 \geq r_1$ by the definition of a generator of a p.r.s. and by the definition of $\underline{R}_i^{\alpha}$. If for some k, $(\underline{r}_{k-2}, \underline{r}_{k-1}, \underline{r}_k)$ is a p.r.t. and $\mathring{r}_k = 0$ or $r_k\delta < \mathring{r}_k$, $(\underline{r}_{k-1}, \underline{r}_k)\underline{R}_i^{\alpha} = \underline{r}_{k-1}$. Hence $(\underline{r}_{k-1}, \underline{r}_k, \underline{r}_{k+1})$ is not a p.r.t. Therefore if $\underline{r} = (\underline{r}_0, \underline{r}_1, \ldots, \underline{r}_n)$ is a p.r.s. and $(\underline{r}_0, \ldots, \underline{r}_n, \underline{r}_{n+1})$ is not, the condition $\mathring{r}_m = r_m\delta$ holds for $1 \leq m < n$.

<4.3.05>
Definition: $\underline{r} = (\underline{r}_0, \underline{r}_1, \ldots, \underline{r}_n)$ is called a conclusive p.r.s. if $\mathring{r}_n = 0$ and/or $r_n = 0$. By the preceding lemma and the definitions of $\underline{R}_i^{\alpha}$, a conclusive p.r.s. must also be normal.

The above definitions and lemmas hold for polynomials in the modeled and model domains since no restriction was placed on the value of α, the modularization level. The important problem to be solved is to find a relation between the two which allows us to make a conclusive decision about the modeled polynomials while performing operations only on their models in the model domain. The specific question we wish to answer is whether two polynomials in J_i^{-1} are relatively prime with respect to x_i.

<4.3.06>
Theorem: Let $\underline{r}_0, \underline{r}_1 \in \underline{J}_i^{-1}$, $\mathring{r}_0 \geq \mathring{r}_1 = r_1\delta > 0$. Then $(\underline{r}_0, \underline{r}_1, \underline{R}_i^{-1})$ generates the p.r.s. $\underline{r} = (\underline{r}_0, \underline{r}_1, \ldots, \underline{r}_N)$

where $N \geq 2$. Let $\underline{s}_m = \underline{r}_m \underline{D}_{M_i}^{-1,\alpha} \in \underline{J}_i^{\alpha}$. Then $\mathring{s}_0 \geq \mathring{s}_1$ and if $\mathring{s}_1 = s_1 \delta_{i,i}^{\alpha}$, $(\underline{s}_0, \underline{s}_1, \underline{R}_i^{\alpha})$ generates the p.r.s. $\underline{s} = (\underline{s}_0, \underline{s}_1, \ldots, \underline{s}_n)$ where $n \leq N$.

Proof: $(\overset{b}{\underline{R}}_i^h) \in VPH_i^{h,\alpha}$ if $0 < \mathring{b} = b\delta_{i,i}^h = \underline{b} D_{M_i}^{h,\alpha} \underline{\delta}_{i,i}^{\alpha}$ by <4.2.22>

Hence

$$(\underline{s}_0, \underline{s}_1)\underline{R}_i^{\alpha} = (\underline{r}_0 \underline{D}_{M_i}^{-1,\alpha}, \underline{r}_1 \underline{D}_{M_i}^{-1,\alpha})\underline{R}_i^{\alpha}$$

$$= (\underline{r}_0, \underline{r}_1)\underline{R}_i^{-1} \underline{D}_{M_i}^{-1,\alpha}$$

$$= \underline{r}_2 \underline{D}_{M_i}^{-1,\alpha}$$

$$= \underline{s}_2$$

$\underline{s}_2 \underline{\delta}_{i,i}^{\alpha} \leq \underline{r}_2 \delta_{i,i}^{-1}$ by <4.2.17>. By induction on m, $(\underline{s}_0, \underline{s}_1, \underline{R}_i^{\alpha})$ generates $\underline{s}$ and $\mathring{s}_{m+1} = \mathring{s}_m - 1$ for $m < n$. $\underline{s}_n \underline{\delta}_{i,i}^{\alpha} = 0$ or $\underline{s}_n \delta_{i,i}^{\alpha} < \mathring{s}_{n-1} - 1$ and consequently the p.r.s. terminates. $\underline{s}_n = \underline{r}_n \underline{D}_{M_i}^{-1,\alpha}$ implies $\underline{s}_n \delta_{i,i}^{\alpha} \leq \underline{r}_n \delta_{i,i}^{-1} = \mathring{r}$. Hence $n \leq N$.

Theorem: (Model Conclusive g.c.d. Theorem). Let $\underline{r}, \underline{s}$ be the p.r.s. of the previous theorem <4.3.06> and let <4.3.07>
$g = g.c.d.\ (r_0, r_1)$. If $\underline{s}$ is conclusive

1) with $\mathring{s}_n = 0$, $s_n \neq 0$ then $g\delta_{i,i}^{-1} = 0$.
2) with $\mathring{s}_n \geq 0$, $s_n = 0$ then $g\delta_{i,i}^{-1} \leq \mathring{s}_{n-1}$.

Proof: Case 1: $\mathring{s}_n = 0$, $s_n \neq 0$: By theorem <4.3.06> $n \leq N$ and hence $n = N$ and $\mathring{r}_N = 0$. Therefore $g\delta_{i,i}^{-1} = r_N \delta_{i,i}^{-1} = 0$ since $r_N \delta_{i,i}^{-1} = -\infty$ would imply $r_n = 0$ and $s_n = r_n \underline{D}_{M_i}^{-1,\alpha} = 0$

which contradicts the case hypothesis.

Case 2: $\mathring{s}_n \geq 0$, $s_n = 0$: r_{N-1} is an associate of the g.c.d. of r_0 and r_1 in J_i^{-1}. Hence $r_{N-1}\delta_{i,i}^{-1} = g\delta_{i,i}^{-1}$ and $r_N = 0$. But $n \leq N$ by theorem <4.3.06> implying $\mathring{s}_{n-1} = \mathring{r}_{n-1} \geq \mathring{r}_{N-1} = r_{N-1}\delta_{i,i}^{-1}$.

Stated less succinctly the model conclusive g.c.d. theorem states that if a model p.r.s. is conclusive and the last remainder is not 0, the original modeled polynomials r_0 and r_1 are relatively prime in the indeterminate x_i. The second condition states that if the last term in the p.r.s. is 0, the g.c.d. of r_0 and r_1 must have a lower degree in x_i than the degree of the second last term.

The model conclusive g.c.d. theorem has much practical significance since it will show that two polynomials are relatively prime when the p.r.s. is conclusive much more rapidly than methods in which a g.c.d. algorithm is applied directly to the modeled polynomials. To get a better grasp of the implications of this theorem we can consider the following set of non-trivial examples:

Notation: <4.3.10> The polynomials will be represented in sequence form as explained in appendix A.

Example: <4.3.105> Find the GCD of $r_0 = 1 + x_1^2$, $r_1 = 3 + x_1$. $g = g.c.d.(r_0, r_1)$. To illustrate a conclusive p.r.s. in which $s_n = 0$, we use $p_0 = 5$.

$$\begin{aligned} \underline{r}_0 &= 1 \quad 0 \quad 1 \quad ,2 \\ \underline{r}_1 &= 3 \quad 1 \quad\quad ,1 \\ &\quad 1 \quad 2 \quad 0 \quad ,1 \\ \underline{r}_3 &= 0 \quad\quad\quad ,0 \end{aligned}$$

$r_3 = 0$ implies that $g\delta_{1,1}^{-1} \leq 1$. We repeat the calculation using $p_0 = 7$.

$$\begin{aligned} \underline{r}_0 &= 1 \quad 0 \quad 1 \quad ,2 \\ \underline{r}_1 &= 3 \quad 1 \quad\quad ,1 \\ &\quad 1 \quad 4 \quad\quad ,1 \\ \underline{r}_2 &= 3 \quad\quad\quad ,0 \end{aligned}$$

This shows conclusively that the two polynomials are relatively prime. The problem for $p_0 = 5$ was that $1 + x_1^2$ factors into $(3 + x_1)(2 + x_1)$ modulo 5.

Example: <4.3.11> The following polynomials which appeared in reference (4), page 588 illustrate a number of problems which may be encountered and at the same time show how effective the model conclusive g.c.d. theorem is.

$$\begin{aligned} a = {} & (-x^3)y^6 + (5x^2)y^5 + (x^3+x^2-7x)y^4 + (-2x^2-2x+3)y^3 \\ & + (x^3-2x^2-2x+1)y^2 + (x^2+6x+5)y + (-x^3-3x^2-3x-1) \end{aligned}$$

$b = \frac{\partial}{\partial y} a$

Let $x_1 = x$, $x_2 = y$. Then the polynomials are represented by

$a =$

*	0	1	2	3
0	-1	-3	-3	-1
1	5	6	1	0
2	1	-2	-2	1
3	3	-2	-2	0
4	0	-7	1	1
5	0	0	5	0
6	0	0	0	-1

$b =$

*	0	1	2	3
0	5	6	1	0
1	2	-4	-4	2
2	9	-6	-6	0
3	0	-28	4	4
4	0	0	25	0
5	0	0	0	-6

Let the prime context sequence be $(p_0 = 5, p_1 = x_1 - 1, \ldots)$.

Then

$\underline{aD}^0_{2,2} =$

*	0	1	2	3	
0	4	2	2	4	,3
1	0	1	1	0	,2
2	1	3	3	1	,3
3	3	3	3	0	,2
4	0	3	1	1	,3
5	0	0	0	0	,2
6	0	0	0	4	,3
	,6				

$\underline{bD}^0_{2,2} =$

*	0	1	2	3	
0	0	1	1	0	,2
1	2	1	1	2	,3
2	4	4	4	0	,2
3	0	2	4	4	,3
4	0	0	0	0	,2
5	0	0	0	4	,3
	,5				

$$\underline{r}_0 = \underline{aD}^1_{2,2} = ((2,2,3,4,0,0,0,4),6)$$

$$\underline{r}_1 = \underline{bD}^1_{2,2} = ((2,1,2,0,0,4),5)$$

$$\underline{r}_2 = (\underline{r}_0, \underline{r}_1)\underline{\rho} = 4 \overset{1}{\circledcirc} ((2,0,2,2,0),4)$$

Since $\underline{r}_2 \underline{\delta}^1_{2,2} = 3 \neq \mathring{r}_2 = 4$, the result is inconclusive. Now we use the prime context sequence $(p_0 = 11, p_1 = x_1 + 10, \ldots)$.

$\underline{aD}^{1}_{2,2} = ((3,1,9,10,6,5,10),6)$

$\underline{bD}^{1}_{2,2} = ((1,7,8,2,3,5),5)$

$\underline{r}_0 = -a\underline{D}^{1}_{2,2}$	=	8	10	2	1	5	6	1 ,6
$\underline{r}_1 = 9 \overset{1}{\odot} (\underline{bD}^{1}_{2,2})$	=	9	8	6	7	5	1	,5
$(\underline{r}_0, \underline{r}_1)\underline{\rho}$	=	8	1	5	6	9	1	,5
$\underline{r}_2' = ((\underline{r}_0, \underline{r}_1)\underline{\rho}, \underline{r}_1)\underline{\rho}$	=	10	4	10	10	4		,4
$\underline{r}_2 = 3 \overset{1}{\odot} \underline{r}_2'$	=	8	1	8	8	1		,4
$(\underline{r}_1, \underline{r}_2)\underline{\rho}$	=	9	0	5	10	8		,4
$\underline{r}_3 = ((\underline{r}_1, \underline{r}_2)\underline{\rho}, \underline{r}_2)\underline{\rho}$	=	0	3	7	1			,3
$(\underline{r}_2, \underline{r}_3)\underline{\rho}$	=	8	1	5	1			,3
$\underline{r}_4' = ((\underline{r}_2, \underline{r}_3)\underline{\rho}, \underline{r}_3)\underline{\rho}$	=	8	9	9				,2
$\underline{r}_4 = 5 \overset{1}{\odot} \underline{r}_4'$	=	7	1	1				,2
$(\underline{r}_3, \underline{r}_4)\underline{\rho}$	=	0	7	6				,2
$\underline{r}_5 = ((\underline{r}_3, \underline{r}_4)\underline{\rho}, \underline{r}_4)\underline{\rho}$	=	2	1					,1
$(\underline{r}_5, \underline{r}_4)\underline{\rho}$	=	7	10					,1
$\underline{r}_6 = ((\underline{r}_5, \underline{r}_4)\underline{\rho}, \underline{r}_4)\underline{\rho}$	=	9						,0

The result is conclusive and indicates that the g.c.d. is independent of y.

If we try to use the $D^{0}_{2,1}$ model to check if the g.c.d. is independent of x_1, an inconclusive result will always occur no matter what the value of p_0. This is caused by the symmetry of the polynomials in the coefficients of x_1^3 which will generate a zero coefficient during summation. $\underline{r}_1 = \underline{bD}^{0}_{2,1}$ will be degree reduced and consequently cannot be used as a divisor in the reduction function.

If it is still desired to continue in the model domain, two alternatives remain. The x_1 and x_2 indeterminates can be interchanged by a substitution operation and a prime sequence, $(p_0, p_1 = x_1 - \beta, \ldots)$ where $\beta \neq 1$ can be used in the modelings: $\underline{r}_0 = \underline{aD}^1_{2,2}$ and $\underline{r}_1 = \underline{bD}^1_{2,2}$. If this still does not destroy the symmetry which causes the cancellation, p_1's of higher degree in x_1 can be used. Alternatively, since it has been established that the g.c.d. is independent of y, the pair-wise g.c.d.'s of the y coefficients can be calculated. This discussion should provide sufficient evidence to indicate that there exist significant problems in determining the best strategy to be used after an inconclusive p.r.s. is encountered in the model domain.

Example: <4.3.12> As a final example, we consider a 36 term, 2 variable, total degree 7 pair of polynomials whose coefficients are decimal digits extracted from a table of random numbers. Collins (6) demonstrated that of the 4 g.c.d. methods he considered only the reduced p.r.s. algorithm was capable of showing similar pairs relatively prime in a reasonable amount of computation time. The prime context sequence is $(p_0 = 7, p_1 = x_1 - 1, \ldots)$.

$a =$

*	0	1	2	3	4	5	6	7
0:	8	4	6	7	8	8	6	1
1:	8	8	4	2	8	9	2	
2:	8	6	0	2	3	5		
3:	6	7	1	5	0			
4:	5	5	5	0				
5:	9	9	3					
6:	7	8						
7:	5							

$b =$

*	0	1	2	3	4	5	6	7
0:	7	7	7	8	6	6	5	6
1:	7	1	5	4	6	6	3	
2:	8	3	6	3	6	3		
3:	9	0	3	1	6			
4:	9	1	7	9				
5:	4	6	6					
6:	3	4						
7:	9							

	0	1	2	3	4	5	6	7	
$\underline{r}_0' = \underline{b}D^1_{2,2}$	3	4	1	5	5	2	0	2	,7
$\underline{r}_1' = \underline{a}D^1_{2,2}$	6	6	3	5	1	0	1	5	,7
$\underline{r}_0 = \underline{r}_0' \odot 4$	5	2	4	6	6	1	0	1	,7
$\underline{r}_1 = \underline{r}_1' \odot 3$	4	4	2	1	3	0	3	1	,7
$\underline{r}_2 = (\underline{r}_0, \underline{r}_1)\underline{\rho}$	2	3	4	3	6	2	1		,6
$(\underline{r}_1, \underline{r}_2)\underline{\rho}$	4	2	6	4	0	1	1		,6
$\underline{r}_3$	5	1	5	6	6	1			,5
$(\underline{r}_2, \underline{r}_3)\underline{\rho}^*$	3	4	1	4	0	1			,5
$\underline{r}_4$	5	3	3	5	1				,4
	5	3	2	3	1				,4
$\underline{r}_5$	0	0	4	1					,3
	5	3	3	1					,3
$\underline{r}_6$	2	4	1						,2
	0	5	0						,2
$\underline{r}_7$	0	1							,1
	4	1							,1
$\underline{r}_8$	1								,0

The result is conclusive and $r_8 \neq 0$ implies that the g.c.d. does not contain a term with x_2.

It should be noticed that if the two polynomials do have a g.c.d. of degree 1 or greater the algorithm in the model domain will always be either inconclusive or have a final remainder of zero in the sequence; s_{n-1} will be a model of the actual g.c.d. but having available only the developments derived previously in this chapter we are not able to calculate the actual g.c.d. from this model.

In a polynomial manipulator the model g.c.d. algorithm should be used as a "filter" which is able to catch most polynomial pairs which are relatively prime, depending on specific values of elements in the prime context sequence. The polynomial pairs which do survive this filtering will very likely have a non-trivial g.c.d. At this point the filtering can either be repeated with a much more refined prime context sequence (e.g. p_0 is larger) or g.c.d. algorithms such as discussed in reference (6) can be applied in the modeled domain.

4.4 On the Use of Augmented Modeling in Elimination

Let $a_k \in I_m$ and let the equation $a_k = 0$ be represented by e_k. The system of equations $E = \{e_k \mid e_k : a_k = 0,\ 0 \leq k \leq n-1\}$ then has n equations in m unknowns which are in general not linearly related.

The elimination method is the orderly application of the reduction operator, ρ, to the equations in the system so as to attempt to reduce the problem to that of finding the zeros of an equation $b = 0$ where $b \in I_1$. For the case in which E is a linear system of equations the method reduces to the commonly used Gaussian elimination in which the system E is represented in matrix form.

The operations used during elimination are similar to those used in finding the g.c.d. of two polynomials and consequently we can expect to be able to generate some conclusive results by operations performed only in the model domains. As an example we will demonstrate the use of augmented modeling as a method for checking the consistency of the system E when E is linear and overspecified in the sense that $n > m$.

Let $e = (e_0, e_1, e_2, e_3)$, $e_k : a_k = 0$, $a_k \in I_3$

$$
e: \quad
\begin{aligned}
e_0&: \quad x_3 + 2x_2 + 3x_1 + 4 = 0 \\
e_1&: \quad 2x_3 + 4x_2 + 5x_1 + 6 = 0 \\
e_2&: \quad x_3 + 9x_2 + 6x_1 + 2 = 0 \\
e_3&: \quad x_3 + 3x_3 + 5x_1 + 1 = 0
\end{aligned}
$$

The above is a system of 4 equations in 3 unknowns in which the initial ordering was made arbitrarily. Since we will have to be able to interchange the ordering, we define the following operator:

Definition: $S^n_{i,j} : (A)^n \longrightarrow (A)^n$; $S^n_{i,j}$ induces a permutation on $(A)^n$ such that for <4.4.01>

$a = (a_0, a_1, \ldots, a_{n-1}) \in (A)^n$, $aK_i = aS^n_{i,j}K_j$ and $aK_j = aS^n_{i,j}K_i$ where the component function K is defined in <2.6.02>.

For convenience we make the following notation conventions:

$e_{2,3} = (e_2, e_3)$; $e_{0,2} = (e_0, e_1, e_2)$; $e = (e_{0,2}, e_3) = (e_0, e_1, e_2, e_3)$.

The system of equations are represented in the matrix form:

$$e: \quad \begin{matrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 5 & 6 \\ 1 & 9 & 6 & 2 \\ 1 & 3 & 5 & 1 \end{matrix}$$

First we generate the $\underline{D}^0_{3,3}$ model of the system with $p_0 = 7$. The V component of the augmented models appears after each comma; only the V components which will be used in the elimination are shown.

$$\overset{0}{\underline{e}} = e\underline{D}^0_{3,3}: \quad \begin{matrix} 1,1 & 2,1 & 3,1 & 4,0 \\ 2,1 & 4,1 & 5,1 & 6,0 \\ 1,1 & 2,1 & 6,1 & 2,0 \\ 1,1 & 3,1 & 5,1 & 1,0 \end{matrix}$$

The application of the elimination method on the system results in the following set of system states:

$$\overset{1}{\underline{e}} = (\overset{0}{\underline{e}}_0, \underline{e}_{1,3}(\underline{\rho})): \quad \begin{matrix} 1,1 & 2,1 & 3,1 & 4,0 \\ 0,0 & 0,1 & 6,1 & 5,0 \\ 0,0 & 0,1 & 3,1 & 5,0 \\ 0,0 & 1,1 & 2,1 & 4,0 \end{matrix} \quad \begin{matrix} \overset{0}{\underline{e}}_0 \end{matrix}$$

degree reduced in x_2 " " " "

$$\overset{2}{\underline{e}} = (\overset{1}{\underline{e}}_0, \overset{1}{\underline{e}}_{1,3} S^3_{0,2}): \quad \begin{matrix} 1,1 & 2,1 & 3,1 & 4,0 \\ 0,0 & 1,1 & 2,1 & 4,0 \\ 0,0 & 0,1 & 3,1 & 5,0 \\ 0,0 & 0,1 & 6,1 & 5,0 \end{matrix}$$

$$\overset{3}{\underline{e}} = (\overset{2}{\underline{e}}_{0,1}, \overset{2}{\underline{e}}_{2,3}(\underline{\rho})): \quad \begin{matrix} 1,1 & 2,1 & 3,1 & 4,0 \\ 0,0 & 1,1 & 2,1 & 4,0 \\ 0,0 & 0,0 & 3,1 & 5,0 \\ 0,0 & 0,0 & 6,1 & 5,0 \end{matrix} \quad \begin{matrix} \overset{2}{\underline{e}}_1 \end{matrix}$$

$$\overset{4}{\underline{e}} = (\overset{3}{\underline{e}}_{0,2}, \overset{3}{\underline{e}}_4(\underline{\rho})): \quad \begin{matrix} 1,1 & 2,1 & 3,1 & 4,0 \\ 0,0 & 1,1 & 2,1 & 4,0 \\ 0,0 & 0,0 & 3,1 & 5,0 \\ 0,0 & 0,0 & 0,0 & 2,0 \end{matrix} \quad \begin{matrix} \overset{3}{\underline{e}}_2 \end{matrix}$$

The last equation in $\overset{4}{\underline{e}}$ states that $2 = 0 (\text{mod } 7)$, a contradiction. $\overset{1}{\underline{e}}$ is degree reduced in its equations $\overset{1}{\underline{e}}_1$ and $\overset{1}{\underline{e}}_2$. Since $\overset{1}{\underline{e}}_1$ should be used as the divisor in the reduction, the method would fail since $\underline{\rho}$ would not be in VPH. By performing an interchange of equations with the operator $S^3_{0,2}$, $\overset{2}{\underline{e}}_1 = \overset{1}{\underline{e}}_3$ is used as the divisor in the reduction which generates $\overset{3}{\underline{e}}$. As a result the entire sequence of operations performed on $\underline{e}$ are all in VPH and consequently theorem <4.2.17> applies. Since equation $\overset{4}{\underline{e}}_3$ is a contradiction, a corresponding contradiction holds when the equivalent sequence of operations in the modeled domain is evaluated. In other words, the above contradiction in the model domain implies that in the modeled domain the rank of the augmented matrix of the linear system E is greater than the rank of the coefficient matrix.

It is of interest to note that the sequence of operations applied in the model system creates an "operation trail" based only on decisions derived from the model system. When this same trail of operations is applied to the modeled system it is guaranteed that the divisor of any reduction operation will not be zero and consequently that the reduction will be performed effectively. This in turn implies that as long as the model operations are valuation preserving homomorphic functions, all sequencing decisions in the elimination algorithm can be made independent of the information in the modeled system.

Though a further study of the applications of augmented modeling has not been made it is expected that its use can be extended to nonlinear systems and to the reduction of systems of differential equations as discussed by Brahns.[2] Also, under the VPH proviso the solutions generated in the model domain are models of the solutions in the modeled domain and consequently if a number of model solutions using different primes are generated, a reconstruction based on the Chinese remainder theorem which generates the solution should be capable of being defined for at least some classes of linear systems. In reference (9) where Moses discusses the practicality of solving systems of polynomial equations by elimination it is brought out that the main problem is the explosive growth of coefficients. Since augmented modelings can be

defined so that the coefficients are elements of finite fields, this growth is completely under control. However, the problem that now presents itself involves determining whether or not sufficient information is still retained in the model to draw conclusive results from it.

CHAPTER V THE PRIME CONTEXT SEQUENCE

5.1 Introduction

In previous chapters the existence of prime context sequences $(p_0, p_1, p_2, \ldots)$ was tacitly assumed. Since the primes in these sequences determine the properties of the modeling we will briefly look into their characteristics and generation. The prime integer p_0 plays the most important role since the rest of the polynomials in the sequence are defined on adjunctions for which p_0 determines the prime subfield.

5.2 p_0

The prime integer p_0 determines the number of elements in the prime subfield and therefore can be used to control the amount of storage required for the models. To maximize the information content in relation to the number of bits of storage in a binary machine, p_0 should be of the form $2^n - m$ where n is the number of bits and m is the smallest odd number which optimizes some other aspect of operations in F_0. These other aspects cannot be specified independent of the particular method and equipment used to perform the operations. For example, if the operations are performed by subroutines in a computer with an unalterable structure, not much of an increase in speed can be achieved by choosing different values of m. However, if the hardware

in the computer is alterable in such a way that it can for example perform ones complement 13 bit arithmetic, addition and multiplication modulo 8191 can be performed very rapidly whereas a choice of $p_0 = 2^{13} - 31$ would require much more time to perform the same operations given the identical hardware configuration. This then is an example of hardware being naturally tuned to a particular p_0.

If the circuitry in the computer's central processor is not rigidly specified, it may be possible to change it dynamically so that it will always be tuned to the particular p_0 being used. This in turn implies that addition and multiplication modulo p_0 can be performed in about the same amount of time required to perform integer addition and multiplication respectively. That this is possible should be apparent by observing that the end around carry in ones complement arithmetic corresponds to the reduction of a number modulo $2^n - 1$. If the prime is $2^n - m$, the end around carry digit is replaced by the addition of m to the least n bit positions of the number. Showing that this results in a valid modulo p_0 operation requires too many details which it is undesirable to introduce at this point. However, we may observe that the circuitry required is minimized if m and consequently p_0 has the least arithmetic weight possible where the arithmetic weight is defined as the number of non-zero digits in the canonical

(sometimes called the non-adjacent) binary recoding of the number. Primes of the form $2^n - m$ with m as small as possible and of least arithmetic weight are tabulated in appendix B for $n = 3$ to $n = 24$.

Though addition and multiplication in modular arithmetic can be relatively simple and fast, the analog of division in integer arithmetic is less trivial since the process requires finding the inverse in F_0 of the divisor and multiplying it with the dividend. Division and inversion do not have the same importance as addition and multiplication in finite field operations, but they are used frequently enough to justify studying the optimization of the relatively complex inversion operation. Since a search of the literature indicated that only table look-up has been employed to any extent for inversion, it seems appropriate that the following theorem be presented:

Theorem: <5.2.01> The following three methods are valid algorithms for the computation of the inverse of $a \in F_0$, $a \neq 0$.

1. (Product Method)

Define b_i, β_i such that $b_i \in \{0,1\}$, $\beta_0 = a$, $\beta_{i+1} = \beta_i \overset{0}{\odot} \beta_i$ and $p_0 - 2 = \sum_{i=0}^{n} b_i 2^i$. Then $a^{-1} = \prod_{i=0}^{n} \overset{0}{\odot} (\beta_i^{b_i})$.

2. (Recursive Method)

If $a = 1$, $a^{-1} = 1$. If $a \neq 1$, define $r_0 = a$ and determine n, q_i from the equation $p = q_i \circ r_{i-1} + r_i$ where n is such that $r_n = 1$. Define $Q_n = 1$, $Q_i = (-q_{i+1}) \overset{0}{\odot} Q_{i+1}$ for $0 \leq i \leq n - 1$. Then $a^{-1} = Q_0$.

3. (Factor Synthesis Method)

If $a \neq 1$, calculate q_i, r_i, Q_i by the iteration

$$p = q_0 \circ a + r_0; \quad Q_0 = r_0 + 1$$

$$a = q_i \circ r_{i-1} + r_i; \quad Q_i = (Q_{i-1} \overset{0}{\oplus} (-1)^i) \overset{0}{\odot} q_i, \quad i > 0.$$

Find n such that $r_{n+1} = 0$. Then

$$a^{-1} = (-1)^{n+1} \overset{0}{\odot} [Q_n \overset{0}{\oplus} (-1)^{n+1}] \overset{0}{\odot} (r_n)^{-1}$$

Proof:

Part 1 is based on Fermat's theorem which states that for any non-zero element, a, in a finite field of order p_0, $a^{p_0-1} = 1$. This implies that the inverse of a is a^{p_0-2}. The proofs for the other two methods depend on induction applied in a direct manner and so are not included.

The most interesting of the three methods of inversion seems to be the recursive method since with it there appears to be the ability of optimizing the procedure by choosing an appropriate p_0 and it also seems to have the

property of requiring fewer operations than the other two inversion methods, particularly if the inversion circuitry is tuned to operations in F_0. Attempts were made to find an analytic result for the maximum and average recursion depth for a particular p_0. This problem appeared to be untractable analytically, so the brute force method in which all non-zero elements in the prime fields generated by selected p_0 of the form $2^n - m$ where n ranged from 3 to 16 were inverted to find the maximum and average recursion depths for these primes. The results of these calculations again did not indicate an asymptotic value which either of the recursion depths approaches. There does seem to be a correspondence between the maximum recursion depth and σ_0, the number of factors in $p_0 - 1$. The calculations seem to indicate that the more factors $p_0 - 1$ has, the smaller the maximum recursion depth can be expected to be. In appendix B the maximum and average recursion depths are listed for some of the tabulated p_0's.

One additional property of the prime subfield which might lead to some interesting results concerns the values of p_0 for which $x_1^2 + 1$ is irreducible. If this is the case, $x_1^2 + 1$ will be a prime polynomial and the variable x_1 in the finite field F_1 will have the property of the complex variable i. This points toward the representation of models involving complex numbers in which i is

represented by x_1. If the polynomial $x_1^2 + 1$ is irreducible, $p_0 - 1$ is referred to as a quadratic non-residue (QNR) and if it is reducible to two linear polynomials, a quadratic residue (QR).[12] This is the reason for providing two primes for each value of n in appendix B.

If a significant portion of a computer's time is to be devoted to polynomial manipulation it is important that the operations modulo p_0 be optimized. Of all the operations in various model domains these prime field operations will be performed most frequently. Consequently it is expected that the speed of the polynomial manipulator will be strongly related to the speed of these prime field operations when finite field based modeling is used.

5.3 p_i, $i > 0$

We have already seen examples of p_i's with $i > 0$. Specifically, $(p_0, p_1 = x_1 - 1, p_2 = x_2 - 1, \ldots)$ defines an elementary prime context sequence in which each of the fields F_i is identically equal to the prime subfield. Although the above is a very degenerate form of prime context sequence, it is expected to be of great practical value, the reasons being that it contains a totally symmetric set of polynomials. If the modeling is performed on a polynomial in several variables and a permutaion of the variables in both the modeled and the model polynomials is performed, the model resulting

from the permutation will be identical to that obtained by applying the modeling function to the permuted modeled polynomial. In this sense the modeling is not affected by the permutation of the variables and of course the new prime polynomial context sequence will be identical to the one used prior to the permutation. Since the permutation of variables may possibly lead to procedures for optimizing some polynomial operations this symmetry property of a prime context sequence might be worth persuing further for other less degenerate sequences. It is also interesting to note that the above elementary prime context sequence produces redundant information which is essentially identical to that produced by the function coding used by Martin.[8]

Finding prime context sequences with polynomials which contain more than a few terms can become quite complicated. Fortunately the finite field theory which has been developed provides us with one main theorem which can be used to calculate non-trivial polynomials for the sequences. The theorem is stated in reference (1) theorem 19, p. 135; what follows is a rephrasal of that theorem using the terminology of the previous chapters.

<5.3.01> Definition: Let $q_i = p_0^{d_0 d_1 d_2 \cdots d_i}$ where $d_0 = 1$ and $d_j = \deg_j(p_j)$. Then $a \in F_i$, $a \neq 0$ is said to

be a primitive element of F_i if $a^{q_i-1} = 1$ and there does not exist a t such that t divides (q_i-1) and $a^t = 1$.

<u>Theorem</u>: Let a be a primitive element of F_i and let t be an integer such that t divides (q_i-1). Let r be another integer such that g.c.d. $(r,t) = 1$. Define $g = $ g.c.d. (r,q_i-1). If 4 divides t we require that $q_i = 1 \pmod 4$. Under these conditions $x_{i+1}^t - a^r$ is an irreducible polynomial belonging to the exponent $\frac{t(q_i-1)}{g}$. <5.3.02>

The properties of polynomials used in the prime context sequence for practical polynomial manipulation require that multiplication in the finite fields be optimized. This in turn dictates that the prime polynomials contain as few non-zero terms as possible. The binomials produced by the above theorem are therefore optimum in this respect.

There are quite a number of open questions related to finding optimum prime context sequences. As an example we can have one sequence in which $p_0 = 2^9-9, p_1 = x_1 - 1$ and another in which $p_0 = 7, p_1 = x_1^3 - 5^2 = x_1^3 + 3$. The elements of F_1 of both sequences contain approximately 9 bits of information, yet the structure of the fields is quite different. The speed of operations performed in F_1 depends very heavily on the choice made. For example, if operations in F_0 require negligible time compared to polynomial operations

in F_1, the first sequence should be chosen. The relative merits depend in general on the particular methods used to implement the polynomial manipulator.

CHAPTER VI CONCLUDING REMARKS

The objectives of this investigation were to find a class of redundancies of polynomials in several variables over the integral domain of integers which would be useful in enhancing the power of polynomial manipulators by increasing their efficiency or their capability of handling more complex problems than are currently possible. The finite field based modeling functions of <3.6.07> and <4.2.08> have been shown capable of doing both. The most illustrative example presented is the application of the augmented modeling method to the determination of the greatest common divisor of two polynomials; it is shown that the method can be used to increase the speed of determining whether two polynomials are relatively prime by possibly orders of magnitude. At the same time the method makes feasible the application of the g.c.d. test to polynomials of a size for which it would be impractical to apply even the best available g.c.d. method without using modeling. The reason for this large decrease in computational effort is that the coefficients in the model polynomials are finite field elements which implies that the amount of storage and manipulative effort required to work with them has a relatively low upper bound. Normally the problem in polynomial manipulation is that the size of the coefficients is not bounded and consequently the storage and manipulative effort required can

rapidly reach values which make it impractical to perform the manipulation even on a fast computer.

Though the modeling can be defined so as to produce conclusive results in most practical cases, it is to be understood that there will always be cases in which the results are not conclusive, a fact which must be borne in mind when polynomial manipulations dependent on decisions made from the models are used. Although much of the information in the polynomial can be retained in its model, the possibility of decisions being based on lost information does exist and hence the models cannot be manipulated blindly without taking this into account. The virtual degree augmentation to the modeling is one example of a technique which may be used to prevent this type of decision error. Inconclusive results may still be encountered, but with the augmentation they are detectable, making it possible to take some remedial actions such as reordering the variables, using a different modeling or even changing the prime context sequence. If none of these actions produce a conclusive result one can always return to the modeled domain and apply the algorithm without using modeling provided of course that this is a practical possibility.

It is postulated that the same techniques as used in the g.c.d. calculation can also be successfully utilized to reduce the computational complexity in elimination and in

the reduction of systems of differential equations; results in this area are expected to be particularly worthwhile in regard to making algebraic manipulation efficient enough to be of more general use than is now the case. Some additional areas in which modeling might prove useful are polynomial factoring, error checking, operation optimization by model determined orderings and printed polynomial output monitoring. There is also the possibility that the modeling can be applied to functions other than polynomials in a manner analogous to the coding used by Martin.[8]

APPENDIX A

On the following page a polynomial in I_3 with 64 terms of one decimal digit each is mapped into all its possible model domains under the prime context sequence $p_0 = 7$, $p_1 = x_1^2-1$, $p_2 = x_2-1$, $p_3 = x_3-1$. The information is compressed in such a way that the polynomial

$$x_1 + (2+3x_1^2)x_2 + (4x_1^2+5x_1x_2+6x_2^2)x_3 + (7x_1+(8+9x_1^2)x_2)x_3^2$$

would be represented by

*	0	1	2
00	0	1	0
1	2	0	3
10	0	0	4
1	0	5	0
2	6	0	0
20	0	7	0
1	8	0	9

An X in a position indicates that the coefficient which should be present is greater than 9.

* indicates the start of a polynomial in J_i^α

α

i = -1

*	0
00	X

i = 0

*	0
00	1

i = 1

*	0	1	2	3
00	X	X	X	X

*	0	1	2	3
00	0	3	6	6

i = 2

*	0	1	2	3
00	X	8	X	X
1	X	X	X	X
2	X	X	X	X
3	7	X	X	X

*	0	1	2	3
00	1	1	1	0
1	1	2	4	1
2	5	4	0	0
3	0	3	1	5

i = 3

*	0	1	2	3
00	6	0	2	6
1	6	3	2	1
2	3	6	7	9
3	1	9	5	8
10	3	2	3	3
1	9	7	6	2
2	0	5	5	2
3	4	5	6	1
20	6	3	9	2
1	1	4	4	5
2	1	0	7	1
3	0	3	4	5
30	0	3	8	3
1	6	2	6	7
2	8	0	2	2
3	2	7	7	5

*	0	1	2	3
00	6	0	2	6
1	6	3	2	1
2	3	6	0	2
3	1	2	5	1
10	3	2	3	3
1	2	0	6	2
2	0	5	5	2
3	4	5	6	1
20	6	3	2	2
1	1	4	4	5
2	1	0	0	1
3	0	3	4	5
30	0	3	1	3
1	6	2	6	0
2	1	0	2	2
3	2	0	0	5

i = 1

*	0	1
00	6	2

*	0	1
00	2	1
1	5	3
2	5	4
3	1	1

*	0	1
00	1	6
1	1	4
2	3	1
3	6	3
10	6	5
1	1	2
2	5	0
3	3	6
20	1	5
1	5	2
2	1	1
3	4	1
30	1	6
1	5	2
2	3	2
3	2	5

i = 2

*	0	1
00	6	2

*	0	1
00	4	0
10	1	6
20	4	2
30	4	1

i = 3

*	0	1
00	6	2

-1	0	1	2	3
	$p_0 = 7$	$p_1 = x_1^2+6$	$p_2 = x_2+6$	$p_3 = x_3+6$

APPENDIX B

Minimum Weight Primes

p_0-1 is a QNR

n	m	w	σ_0	MR	AVR
3	1	2	4	2	1.17
4	5	3	4	4	1.90
5	1	2	8	5	2.30
6	5	3	4	7	4.29
7	1	2	12	7	3.34
8	5	3	8	12	5.79
9	9	3	4	14	7.97
10	5	3	4	16	8.52
11	9	3	4	17	9.24
12	5	3	8	15	7.09
13	1	2	48	15	6.17
14	65	3	8	22	10.57
15	49	4	32	20	9.95
16	17	3	16	24	11.71
17	1	2	32		
18	5	3	8		
19	1	2	64		
20	5	3	32		
21	9	3	4		
22	17	3	4		
23	1	2	32		
24	5	3	8		

p_0-1 is a QR

n	m	w	σ_0	MR	AVR
3	3	2	3		
4	3	3	6	3	1.50
5	3	3	6	4	2.43
6	3	3	12	6	2.63
7	15	3	10	9	4.11
8	15	3	20	8	3.62
9	3	3	6	11	5.61
10	3	3	24	13	5.60
11	31	3	36	12	5.30
12	3	3	24	15	6.60
13	31	3	48	16	6.78
14	3	3	72	16	6.73
15	19	4	12	21	9.39
16	15	3	120	19	7.88
17	31	3	144		
18	11	4	18		
19	31	3	48		
20	3	3	96		
21	31	3	16		
22	3	3	72		
23	15	3	10		
24	3	3	48		

$p_0 = 2^n - m$

w = arithmetic weight of p_0

σ_0 = number of factors in p_0-1

MR = maximum recursion depth in recursive inversion method

AVR = average recursion depth

REFERENCES

[1] Albert, A. A., "Fundamental Concepts of Higher Algebra", Univ. of Chicago Press, Chicago, Ill., 1956.

[2] Brans, C. H., A computer program for non-numerical testing and reduction of algebraic differential equations, J. ACM 14, 1 (Jan. 1967) p. 45-62.

[3] Brown, W. S., Hyde, J. P. and Tague, B. A., The ALPAK system for non-numerical algebra on a digital computer--II: Rational functions of several variables and truncated power series with rational function coefficients, Bell Sys. Tech. J. 43 (March 1964), p. 785-804.

[4] Collins, G., PM, a system for polynomial manipulation, Comm. ACM 9, 8 (Aug. 1966), 578-589.

[5] Collins, G. E., Polynomial remainder sequences and determinants, Amer. Math. Mon. 73, 7 (Aug.-Sept.) p. 708-712.

[6] Collins, G. E., Subresultants and reduced polynomial remainder sequences, J. ACM 14, 1 (Jan. 1967) p. 128-142.

[7] Garner, H. L., The residue number system, IRE Trans. on Electr. Comp., EC-8, (June 1959) p. 140-147.

[8] Martin, W. A., Hash-coding functions of a complex variable, Artificial Intelligence Project Memo 70, MIT, Cambridge, Mass. 1964.

[9] Moses, J., Solution of systems of polynomial equations by elimination, Comm. ACM 9, 8 (Aug. 1966) p. 634-637.

[10] Paley, H. and Weichsel, P. M., "A First Course in Modern Algebra", Preliminary Edition, Holt, Rinchart and Winston, Inc., New York, 1963.

[11] Van Der Waerden, B. L., "Modern Algebra", Vol. I, Ungar Publishing Co., New York, 1953.

[12] Vinogradov, I. M., "Elements of Number Theory", Dover Publications, Inc., 1954.

VITA

Stephen John Nuspl was born in Stanisic, Yugoslavia, on February 25, 1940. He received a B.A.Sc. degree in Electrical Engineering from the Assumption University of Winsor, Windsor, Ontario in June, 1963. Since then he has attended the University of Illinois and has held a research assistantship in the Department of Computer Science. He is a member of Phi Kappa Phi, the Institute of Electrical and Electronics Engineers and the Association for Computing Machinery.